软件配置手册

Hammer3100 VDSL 系列交换机

发布版本：V1.32

发布日期：2003 年 7 月

港湾网络有限公司
E-mail：customer@harbournetworks.com
http://www.harbournetworks.com

声明

本手册总体上较为全面地包含了该产品目前的功能特性和配置内容，如遇到产品的某些临时变化，或针对用户的某些特殊需求而采取的一些特殊变动，港湾网络有限公司保留继续使用该手册，并以其他方式通知用户的权利。

前言

本前言说明了此文档的大致内容、组织方式、针对用户类型、图标含义和所包含的其他文档的说明。

文档内容

本手册主要是针对 HammerOS 操作系统编写的。HammerOS 系统由港湾网络有限公司自行独立开发，可以运行在 FlexHammer、μHammer、BigHammer 系列交换机、Hammer10000 IP-DSLAM 接入交换机、Hammer3100 VDSL 系列交换机以及 AeoHammer 无线访问设备上。本手册对 HammerOS 针对 Hammer3100 的特性和配置命令进行了详细说明，并对操作系统的一些缺省配置环境加以介绍，同时提供了一些典型的实用配置案例。

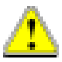
组织方式

本文档主要由以下几个部分组成：

章	题目	内容描述
第 1 章	HammerOS 概述	简述了 HammerOS 的特性，以及 VLAN、Load Sharing、STP 等技术在 Hammer3100 VDSL 系列交换机上的应用。
第 2 章	访问交换机	主要讲述 HammerOS 系统的命令语法、用户权限的设置以及管理交换机的途径等。
第 3 章	配置端口	讲述了 Hammer3100 系列交换机端口的基本参数配置，并针对如何配置多端口负载均衡组（Load Sharing）和端口镜像作了详尽的讨论。
第 4 章	虚拟局域网 VLAN	详细介绍了 VLAN 的作用、分类以及在 Hammer3100 系列交换机中如何完成对 VLAN 各项的配置。
第 5 章	FDB 表	讲述了 FDB（Forwarding Database）地址表的内容和相关知识，以及如何在 Hammer3100 系列交换机上配置静态 FDB 地址表。
第 6 章	STP 协议	主要讲述 STP 协议、如何进行与 STP 相关的配置，以及显示 STP 状态的相关命令。
第 7 章	IGMP Snooping 配置	主要讲述 IGMP Snooping 的配置
第 8 章	SNTP 协议	主要讲述 SNTP 协议、如何进行与 SNTP 相关的配置，以及显示 SNTP 状态的相关命令。

第 9 章	NAS 接入服务	主要讲述网络访问服务器（Network Access Server，NAS）接入服务用户配置
第 10 章	日志模块(Syslog)配置	介绍日志系统的功能以及如何使用。
第 11 章	利用 Web 管理 Hammer3100 系列交换机	主要讲述如何通过 Web 来对 Hammer3100 系列交换机进行配置操作：包括登录、端口配置、VLAN 配置、FDB 地址表配置、STP 的配置、多端口负载均衡组的配置、用户访问权限的设置，以及如何查看相关的系统信息。
第 12 章	启动选项和软件升级	介绍了 Bootrom 启动选项的内容及其含义，如何对系统软件进行升级。

图标说明

图标	说明	
	注意	提示用户在操作过程中需要注意的地方。
	提示	表示给用户提示的附加说明信息。

针对用户类型

本手册主要是针对那些需要使用港湾网络有限公司 Hammer3100 系列交换机实现网络配置和管理的用户或系统管理员，因此要求读者须熟悉以下知识：

- 本地局域网 (Local Area Networks，LAN)
- 以太网概念(Ethernet Concepts)
- 以太网交换和桥概念(Ethernet Switching and Bridging Concepts)
- 网络协议概念(Internet Protocol Concepts)
- 网络数据包交换概念（Internet Package Exchange Concepts）
- 简单网络管理协议概念（Simple Network Management Protocol，SNMP）
- 因特网组播管理协议（Internet Group Management Protocol，IGMP）
- 甚高速数字用户环路（Very-high-bit-rate-Digital-Subscriber Loop，VDSL）

相关文档

Hammer3100 系列交换机的文档部分主要包括：

1.《软件配置指导手册—— Hammer3100 VDSL 系列交换机》 (本文档)

2.《硬件安装指导手册—— Hammer3100 VDSL 系列交换机》

目录

第1章 HammerOS 概述

HammerOS 是港湾网络有限公司专为 Hammer 系列产品设计的操作系统，它可以运行在 FlexHammer、BigHammer、μHammer 系列交换机、Hammer10000 IP-DSLAM 接入交换机和 Hammer3100 VDSL 系列交换机上。

本文档所支持的 Hammer3100 系列交换机包括硬件版本为 1.xx 和 2.xx 的 Hammer3100 交换机和 Hammer3100-16 交换机。

提示：本文档对 Hammer3100 VDSL 系列交换机的软件配置进行了统一讲述；如果涉及到各个产品的特殊配置，将在手册中单独说明。

1.1 特性概述

Hammer3100 系列交换机的特性如下：

- 支持IEEE802.1Q和802.1P标准的Virtual Local Area Networks（VLAN）
- 支持IEEE802.1D标准的Spanning Tree Protocol（STP）
- 线速（Wire-Speed）二层交换
- 支持端口捆绑（Load Sharing）
- 支持网络组管理协议监听Internet Group Management Protocol（IGMP）Snooping
- 支持Console 命令行配置
- 支持Telnet 命令行配置
- 支持Web-based Management
- 支持Simple Network Management Protocol (SNMP)
- 支持VDSL相关特性

1.2 VLAN

Hammer3100 系列交换机的 VLAN 功能使您在构建自己的广播域时，不再受限于网络的物理连接。一个 VLAN 就是一群独立于具体网络拓扑的设备，它们在通讯时，不论如何连接，属于这一 VLAN 的所有设备都好像在一个真正的物理局域网上。VLAN 的具体作用体现在：

可以控制广播数据，限制其广播的范围。假设在 VLAN“研发部”中的一个设备发出了一个广播报文，那么只有“研发部”这个 VLAN 中的设备才能收到该广播报文。其他部门将不会收到该广播报文。

提供了额外的安全特性。跨 VLAN 的访问只有通过三层转发，不能直接访问。例如 VLAN“市场部”的设备只能通过路由协议同 VLAN“研发部”进行通讯。

简化了设备在网络中的移动和管理。具体来讲，VLAN 技术是为了创建第三层逻辑广播域，VLAN 可在一个交换机上划分，也可以跨越多个交换机划分。VLAN 实现了在物理上是一个网

段的交换机群之间进行逻辑 VLAN 划分，即分成多个逻辑广播域，避免广播风暴的发生。

提示：有关 VLAN 的详细配置信息见本文档第 4 章。

1.3 STP（Spanning Tree Protocol）

Hammer3100 系列交换机支持 IEEE802．1D 标准的 STP 协议，这一协议提供了网络的动态冗余切换机制。因此，使用 STP 可以让您在网络设计中部署备份线路，并且保证：

- 在主线路正常工作时，备份线路是禁用的。
- 当主线路出现故障时，自动激活备份线路，将数据流切换到备份线路，保证设备正常运行。

由此可见，使用 STP 可以保证在网络结构存在冗余路径情况下，阻止网络回路状态发生。网络回路对网络来说是致命的打击，冗余链路作为网络备份路径又是非常主要的。STP 是运行在 Bridges 和 Switches 层上并与 802．1D 协议标准兼容的第二层协议。

为了实现上述功能，STP 要求每个 VLAN 都含有一个“Root Switch”，保证 VLAN 中的所有交换机并不处于同等地位的环上，而是处于具有不同优先级的树结构之上。

提示：有关 STP 的详细配置信息见本文档第 6 章。

1.4 Load Sharing

Load Sharing 技术是一种将网络流量聚集在一组端口上的方法，它可以形成一个交换机之间的大容量通道或容错通道，通道之间可以实现流量均衡。

Hammer3100 系列交换机支持 Load Sharing 功能，通过创建 Load Sharing 来提升交换机之间的带宽。Load Sharing 把多个物理端口捆绑在一起当作一个逻辑端口来使用。

其作用表现在以下几个方面：

- 如果Load Sharing中的一个端口发生堵塞或故障，那么数据包会被重新分配到该Load Sharing中别的端口中进行传输。
- 如果这个坏掉的端口重新恢复正常，那么数据包将重新分配到该Load Sharing中的所有端口来进行传输。

Hammer3100 系列交换机的 Load Sharing 功能与 Intel 和 Cisco 的同类产品的 Port Group 功能兼容。

提示：有关端口 Load Sharing 的详细配置信息见本文档第 3 章内容。

1.5 IGMP Snooping 网络组管理协议监听

IGMP（Internet Group Management Protocol ）网络组管理协议是 IP 协议簇中的一部分，用来支持和管理主机与组播路由器之间的 IP 组播。组播允许进行资源发现，使网络负载减到最小，在网上实现数据的有效传输。

IGMP Snooping 用来监听主机与路由器之间的 IGMP 报文,并对监听到的 IGMP 报文进行处理。IGMP Snooping 使交换机能够跟踪与之物理相连的网络上每个组的成员。它在主机和直接邻接的组播路由器间运行，管理组成员关系。

提示：有关端口 IGMP Snooping 的详细配置信息见本文档第 7 章内容。

1.6 支持 SNTP（Simple Network Time Protocol）协议

SNTP 的全名为简单网络时间协议，它是设计来使网络中的设备能维持相同时间的一种通信协议，通过在网络设备中运行 SNTP 协议，有利于网络中设备的管理和维护。

提示：有关 SNTP 协议的详细信息见本文档第 8 章。

1.7 NAS 接入服务

港湾网络有限公司通过在 Hammer 系列交换机上嵌入接入服务完成用户的认证和管理功能。嵌入了接入服务的 Hammer 交换机称为网络访问服务器（Network Access Server，NAS）。

Hammer3100 系列交换机的接入服务在运用 802.1x 协议和 RADIUS 协议的基础上，实现对用户接入的认证和管理功能。

提示：有关 NAS 接入服务方面的详细内容参阅本文档第 9 章。

1.8 Syslog 日志模块

日志模块主要用来记录整个系统的运行情况以及用户操作行为。完整的日志模块能够帮助管理员及时了解和监控系统的工作情况，并实时记录系统的异常信息。

☞**提示：有关 Syslog 方面的信息请参阅本文档第 10 章。**

第2章 访问交换机

本章内容主要涉及管理 Hammer3100 系列交换机所需要的一些知识，包括：

- 理解命令语法
- 行编辑命令
- 历史命令使用
- 一些常用命令
- 设置访问权限
- 管理交换机的途径
- 配置SNMP
- 配置静态路由
- 存取配置文件
- 检测网络基本连接

注意：

如果您想使对设备的配置内容在设备重新启动或关机再开启后仍能有效，请切记在进行配置后使用“ save configuration ”命令把配置保存到设备中。具体请参见本章稍后关于常用命令的介绍。

2.1 理解命令语法

这一节主要讲述通过命令行配置 Hammer3100 系列交换机时对命令语法的理解和使用，请仔细阅读本节以及后边几节中关于使用命令行接口的详细信息。

2.1.1 命令输入规则

使用命令行接口 Command Line Interface（CLI）输入命令，请按照以下步骤进行：

第一步：进入命令行接口，当出现命令提示符后，请确认您有登录 HammerOS 的相应权限。

Hammer3100 系列交换机操作系统包含两种不同权限：一种是管理员权限，拥有对所有命令的配置权；另一种是普通用户权限，没有配置权，只有对部分内容的查看权。同时，Hammer3100 还设有两种管理模式：只读模式和配置模式。在只读模式下只有对接入交换机配置信息的查看权，而在配置模式下除了可以查看接入交换机的所有配置信息以外，还拥有对接入交换机的配置管理权。具有管理员权限的用户能够在这两种模式下操作，而具有普通用户权限的用户只能在只读模式下操作。

如果以普通用户身份登录，您只能在只读模式下操作，命令提示符为“ Harbour> ”。如果以系

统管理员身份登录，您在两种模式下均可以操作，如果是在配置模式下，命令提示符为“ Harbour(config)# ”。

提示：

首次登录请用系统缺省用户帐号，该帐号为管理员帐号，用户名：admin，密码：harbour。

第二步：键入命令名称。

如果键入的命令不含有任何需要用户输入的参数，请直接跳到第三步。如果键入命令中含有需要用户输入的参数，则继续以下步骤。

- 如果命令需要输入一个参数值，请输入这个值。在输入参数值时，可能需要输入关键字。命令的参数值部分一般指定了您应该输入什么样的参数，例如该参数可能是某个范围内的整数值，或者是一个字符串，或者是一个IP地址等等。关键字是指命令中要操作的对象。
- 如果命令需要输入多个参数值，请按命令的提示依次输入关键字和每个参数值，直到提示信息中出现<cr> Just Press Enter to Execute command! 按回车键信息为止

第三步：请按回车键执行命令。

【举例 1】 用户不需要输入参数的情况：

Harbour(config)# exit

“ exit ” 是一个不含参数和关键字的命令。命令名称为 exit。当键入此命令后，按回车则执行该命令。

【举例 2】 用户需要输入参数的情况：

```
Harbour(config)#config  port  2，3  speed 10
```

这是一个含有参数和关键字的命令。

其中，命令名称为 config，关键字为 port 和 speed，参数值为 2，3 和 10。

提示：

当用户输入错误的命令或参数时，系统会给予提示信息，通知用户错误的原因。但有两种情况例外，那就是字符“ ！ ”和“ ＃ ”。HammerOS 系统规定，字符“ ！ ”和“ ＃ ”后面的所有内容均为注释信息，不作为配置命令的一部分。因此，当您输入配置命令时，如果在命令当中的某个空格后输入了“ ！ ”或者“ ＃ ”，那么该字符后的内容将不被处理，此时系统则认为您输入的命令不完全。如果

是在命令的最开始处输入了“ ！ ”或者“ ＃ ”，则相当于没有输入命令。

2.1.2 语法帮助

1.“ ？ ”的使用

命令行接口中内置有语法帮助。如果您对某个命令的语法不太确定，请输入该命令中您所知道的前面部分，然后键入“？”，此时命令行会提示您该命令的含义或作用，如果您在命令的后面输入“ 空格 ＋ ？ ”，此时命令行会提示您在已经输入的部分命令之后可能出现的命令清单。您可以根据其中的提示继续输入命令，直至出现

<cr> Just Press Enter to Execute command!

该提示信息表明命令输入完毕，按回车执行所键入的命令。

【举例】 获取 who 命令的帮助信息

第一步：键入命令：

Harbour>who

第二步：

- 如果接着键入“ ？ ”，系统显示如下信息：

  who   Display who is connected to the switch.

  此信息说明 who 命令所要完成的功能；

- 如果接着输入“ 空格 ＋ ？ ”，系统显示如下信息：

  am   Display me myself who is connected to the target machine.

  <cr>   Just Press Enter to Execute command!

  此信息说明 who 后面可以继续键入 am 构成新的命令，或者直接按回车键执行 who 命令。

2．help 的使用

系统给用户设置了帮助信息，获取此信息，键入命令：

Harbour> help

HammerOS provides help feature as described blow.

1. Anytime you need help, just press "?" and don't

press Enter,you can see each possible command argument

and its description.

2. You can also input "list" and then press Enter

to execute this helpful command to view the list of
commands you can use.

根据提示信息得知可通过以下两种方法获得 HammerOS 提供的帮助信息：

1）在命令行中输入“ ？ ”号，不需按回车键，就可以看到每一个可能的命令参数以及相应的命令功能描述。

2）键入命令 list，按回车键，系统将显示当前命令模式下所有的命令清单，您可以从中选择需要的命令。

2.1.3 使用语法帮助补齐命令

HammerOS 提供对命令进行补齐的功能。当您输入了一部分命令后，然后输入“ Tab ”键，如果匹配的命令有多个，则列出可能的命令清单，如果匹配的命令只有一个，那么命令行会自动把用户输入的那部分命令补齐，并把光标移至最后。

【举例 1】 对 show 命令进行语法补齐

第一步：只键入命令 show 的前两个字母“ sh ”

```
Harbour>sh
```

第二步：接着按“ Tab ”键，系统会将这个命令补齐，如下所示：

```
Harbour>show
```

【举例 2】 对 show 命令进行语法补齐

第一步：键入命令 show

```
Harbour >show
```

第二步：再输入一空格键，然后按”Tab”键，系统会显示如下信息：

```
802.1x     arp       dot1p       fdb        history      idle-timeout
igmp       ip        ipfilter    mirroring  modem        port
services   sharing   sntp-client stpd       syscontact   syslocation
time       vdsl      version     vlan
```

以上信息就是命令 show 之后可以继续输入的命令，然后按系统的提示信息继续键入您需要的命令。

2.1.4 命令简写

命令简写是指您可以只输入命令单词或关键字的前边部分字母，只要那部分字母不会造成歧义，交换机就能够识别该命令，用户可以直接回车执行该命令。但需要用户输入的参数如 VLAN 的名字（如例子中的 market）等，则要求完整输入。

【举例 1】将端口 1-5 以 untagged 的方式加入到 market 虚拟局域网中，键入命令：

```
Harbour(config)#config vlan market add port 1-5 untagged
```

上述命令也可简写为：

```
Harbour(config)#con vl market ad po 1-5 un
```

这两条命令完成的功能相同。

提示：

当使用命令简写时，您必须输入足够多的字母，以确保在交换机的众多命令中不会造成歧义。

2.1.5 端口的表示方法

命令语法中使用参数<portlist>来表示 Hammer3100 系列交换机的端口，可以有以下几种表示方法：

- 表示一个单独的端口

例如：port 3 表示端口 3。

- 表示一个连续范围内的端口，用符号“ - ”

例如：port 1-4 表示从端口 1 到端口 4 这 4 个端口。

- 表示多个端口，中间用逗号隔开

例如：port 1-4，5，8 表示端口 1、2、3、4、5、8。

2.1.6 命令中的符号

您可能会在命令语法中看到各种符号，这些符号只是说明您该如何输入该命令，但不是命令本身的一个部分。表 2-1 对这些符号进行了概要说明。

表 2-1：命令行中的符号

符号	描述
尖括号 <>	尖括号表示此部分必须输入一个参数，该参数可以是字符串、数值范围、IP 地址、端口列表等。 例如命令 create vlan <name>，其中必须在<name>的位置中输入一个合法的字符串作为您所创建的 VLAN

	的名字。 当输入的参数超过允许的范围时，系统将拒绝执行这条命令，并显示“Unknown Command”作为提示信息。
中括号 [ ]和竖直线 |	中括号一般和竖直线配合使用。中括号括起来的部分表示这部分命令有几个用竖直线分隔开的可选项，您必须选择输入其中一项。 例如命令：service telnet[enable|disable] 其中，中括号内包含由竖直线分隔的两个可选项，您必须输入 enable 或者 disable。如果中括号中只有一个可选项，那就直接输入那个可选项即可。
大括号 { }和星号 *	大括号一般和星号配合使用。大括号括起来的部分表示这部分命令可以不输入，也可以重复输入。重复输入的次数由大括号后紧跟的那个星号后的数字指定。 例如命令：show vlan {<name>}*1 表示您可以直接输入 show vlan ，也可以在 show vlan 后加上已经创建的某个 VLAN 的名字。 大括号中的命令可以输入 0-n 次。这个 n 的值由星号后的数字指定。此例中 n＝1，表示<name>参数可以出现 1 次。

2.1.7 命令参数类型

一般以尖括号“< >”括起来的部分是命令参数。HammerOS 的命令参数共有以下四种类型。

数值范围：

当尖括号中是两个数值由减号连接时，表示该参数是取值范围在那两个数值之间的某个数。

例如：<1-255>表示用户可以输入大于等于 1 并且小于等于 255 之间的任意一个整数，比如 2 就是一个合法的数字。

IP 地址：

当尖括号中是 A.B.C.D 时，表示该参数是一个 IP 地址，您必须输入一个合法的 IP 地址值。例如：192.168.0.1 就是一个合法的 IP 地址值。

端口列表：

当尖括号中是 portlist 时，表示该参数是输入端口列表。端口列表中的多个端口之间用逗号“，”分隔，如果是连续的多个端口可以用该连续端口的最小端口号加上减号“-”和最大端口号来表示。

例如：输入 1，3-6，8 表示的端口列表为：1，3，4，5，6，8 。

字符串：

当尖括号中所列的不是以上三种情况时，可能表示该参数需要输入的是一个字符串或者是一个

16 进制的数，具体可以在输入命令到该参数部分时，输入“ 空格+？ ”键查看该部分参数的命令说明。

例如：<macaddr> 表示要输入的是一个 16 进制的 MAC 地址，输入 005023344325 为一个合法的 MAC 地址，<name>则表示要输入一个字符串作为某个对象的名字。

2.1.8 行编辑命令

表 2-2 列出了在命令行中可以使用的行编辑命令。

表 2-2：命令行中的行编辑命令

符号	描述
BackSpace 键或 Del 键或 Ctrl+h	向左删除一个字符
向上箭头键或 Ctrl+p	调用上一个历史命令
向左箭头键或 Ctrl+b	将光标向左移动一格
向右箭头键或 Ctrl+f	将光标向右移动一格
向下箭头键或 Ctrl+n	如果前边使用过向上箭头调用上一个历史命令的,再单击向下箭头键可以显示下一个历史命令。
Ctrl+a	将光标移动到行首
Ctrl+e	将光标移动到行尾
Ctrl+d	将光标所在位置的字符删除
Ctrl+k	将光标以后的字符全部删除
Ctrl+t	将光标所在的字符和光标左边的那个字符互相调换，并将光标向右移动一格
Ctrl+u	整行删除
Ctrl+w	将光标左边的字符全部删除

提示：

上述命令中的 Del 键、向上箭头键、向左箭头键、向右箭头键和向下箭头键命令只支持利用 Telnet 来配置交换机的方式，不支持串口配置。而命令 Ctrl+h、Ctrl+p、Ctrl+b、Ctrl+f 和 Ctrl+n 对上述两种登录方式均支持。

2.1.9 历史命令（history）的使用

HammerOS 能记住用户最近输入的 20 个历史命令。您可以使用 show history 命令来显示已经输入过的命令清单，最多显示 19 条命令，这是因为 show history 命令本身也作为 20 个历史命令之一。您可以通过 Ctrl+b 或 Ctrl+n 键调用上一个或下一个历史命令，其操作方法请见上表 2-2。

【配置实例】显示最近使用过的历史命令

```
Harbour> show history
list
ex
list
show fdb mac
show fdb mac 00:01:10:55:10:19
show fdb vlan
show vlan
show fdb vlan
show fdb vlan uplink
show fdb agingtime
show fdb
```

2.2 常用命令

这节主要讲述命令行中常用的一些命令，特定功能的命令将在以后的章节专门讲述。HammerOS 的命令行提供了两种操作模式，一种是只读模式，另一种是配置模式。在只读模式下用户可以查看大部分系统配置信息，在配置模式下用户能够查看所有系统配置信息，并能修改系统配置。

表 2-3：命令行操作模式

操作模式	描述	命令提示符
只读模式	查看部分系统配置信息	以“ > ”结尾，Harbour>
配置模式	查看、修改所有系统配置信息	以“ # ”结尾 Harbour(config)#

从只读模式进入配置模式的命令为“ enable ”，操作如下：

```
Harbour>enable
password：
```

输入进入配置模式密码后按回车便可进入配置模式，其显示为：

Harbour(config)#

退回上一级命令模式，使用命令：exit

2.2.1 show version

【命令作用】显示 Hammer3100 系列交换机系统的软件和硬件版本号及出厂日期等信息。

【命令语法】show version

【命令模式】只读模式和配置模式

【配置实例】

```
Harbour (config)# show version
HammerOS Version1.32 Release3.7.0 on Hammer3100.

Hardware Version: Version 1.33
Software Version: Version1.32 Release3.7.0(Compiled Jun 27 2003 10:48:04)
Manufacture Date: 2002-07-19
Serial    Number: 01010035A133027000298
Base Mac Address: 00053b500330

Copyright(c) 2001-2002 by Harbour Networks, Ltd.
```

2.2.2 enable

【命令作用】由只读模式进入配置模式

【命令语法】enable

【命令模式】只读模式

【配置实例】由只读模式进入配置模式

```
Harbour> enable
Password：
Harbour(config)#
```

2.2.3 terminal length

【命令作用】设置终端每屏显示的行数。

【命令语法】terminal length <0-512>。

【使用指导】length 指定的行数，范围从 0 至 512。缺省配置为每屏显示 20 行。如果将参数 length 设为 0，则表示对每屏显示的行数不作限制。

【命令模式】只读模式和配置模式

2.2.4 help

【命令作用】输出关于怎么使用“？”寻求帮助提示的文字。

【命令语法】help

【命令模式】在任意模式下均可执行。

【配置实例】使用 help 命令

```
Harbour(config)# help

HammerOS provides help feature as described blow.

      1. Anytime you need help, just press "?" and don't
  press Enter,you can see each possible command argument
```



```
and its description.

    2. You can also input "list" and then press Enter
to execute this helpful command to view the list of
commands you can use.
```

该提示信息大意如下：

- 通过以下两种方法，可以获得HammerOS提供的帮助信息：
- 在命令行中输入“ ? ”号，不需按回车键，就可以看到每一个可能的命令参数以及相应的命令功能描述。
- 键入命令list，按回车键，系统将显示所有在当前命令模式下的命令清单，您可以从中选择需要的命令。

2.2.5 who

【命令作用】显示当前有哪些用户连接到目标机器。

【命令语法】who

who am i

【命令模式】只读模式和配置模式

【使用指导】命令 who 显示所有连接到交换机的用户信息，而命令 who am i 只显示自己的信息。

【配置实例】

```
Harbour(config)# who
SessionID. - UserName ---------- LOCATION ---------- MODE ----
5            admin          console       CONFIG     (That's me.)
Total 1 sessions in current system.

Harbour(config)# who am i
I am *Session [5] : user admin connected from console.
```

2.2.6 list

【命令作用】显示当前模式下的所有命令及其相应参数。

【命令语法】list

【命令模式】只读模式和配置模式

2.2.7 list <pattern>

【命令作用】显示指定字符串的命令，通过此命令可以快速查找所需要的命令信息，该命令将列出所有包含给定字符串的命令。

【命令语法】list <pattern>

【命令模式】只读模式和配置模式

【配置实例】

```
Harbour(config)# list create
create fdbentry <macaddr> <portlist> {<vlanname>}*1
create ipfilter [<A.B.C.D/M> | <A.B.C.D/A.B.C.D>] [permit|deny]
create ipfilter ipaddress <A.B.C.D/M> [permit|deny]
create ipfilter ipaddress <A.B.C.D> <A.B.C.D> [permit|deny]
create sharing <mainport> grouping <portlist> {[SourceDestination]}*1
create telnet_filter [<A.B.C.D/1-32> | <A.B.C.D/A.B.C.D>] [permit|deny]
create vlan <name>
```

2.2.8 show services

【命令作用】显示系统 Services 状态，包括 Telnet、SNMP Agent、SNMP Trap 和 Web Manage。

【命令语法】show services

【命令模式】在任意模式下均可执行。

【配置实例】

```
Harbour(config)# show services
Service telnet is up.
Service snmp agent is down.
Service snmp trap support is down.
Service Web manage is down.
```

2.2.9 save configuration

【命令作用】把当前正在运行的配置写到设备的 Flash 中并保存。

【命令语法】save{configuration}*1

【命令模式】配置模式

【使用指导】如果您想让当前所作的配置在设备断电或重新启动后依然有效，切记一定要事先使用此命令保存您的配置。

2.2.10 quit

【命令作用】退出和目标机之间的连接。

【命令语法】quit

【命令模式】只读模式和配置模式

【使用指导】命令 quit 与命令 logout 作用相同。

【配置实例】

```
Harbour(config)# quit
Quit.
Disconnected.
Thanks for using Harbour Networks's product.
Bye!
```

```
##############################################################
#                                                            #
#                  Welcome to HammerOS.                      #
#                                                            #
#        Press Return to connect and config this system.     #
#                                                            #
##############################################################
```

【相关命令】logout

2.2.11 logout

【命令作用】退出和目标机之间的连接，并直接退出命令行。

【命令语法】logout

【命令模式】只读模式和配置模式

【使用指导】命令 logout 与命令 quit 作用相同。

【配置实例】使用 logout 命令

```
Harbour(config)# logout
Quit.
Disconnected.
Thanks for using Harbour Networks's product.
Bye!


##############################################################
#                                                            #
#                  Welcome to HammerOS.                      #
#                                                            #
#        Press Return to connect and config this system.     #
#                                                            #
##############################################################
```

【相关命令】quit

2.2.12 show idle-timeout

【命令作用】显示 idle timeout（空闲超时）时间。

【命令语法】show idle-timeout

【命令模式】只读模式和配置模式

【使用指导】空闲时间是指在此时间段内未对系统作任何操作，使用 idle-timeout <0-35791> 命令可以指定空闲时间，超过这个时间后，退出系统并断开与交换机的连接。

【配置实例】

Harbour(config)# show idle-timeout

```
Idle time out is set to 10 minutes
```

【相关命令】idle-timeout

2.2.13 erase

【命令作用】擦除本交换机中保存的启动配置信息

【命令语法】erase {startup-config}*1

【命令模式】配置模式

【配置实例】

```
Harbour(config)# erase startup-config
Are you sure want to erase startup-config? [Y/N]y

Trying erase all configuration from flash, please wait ...... finished。
Successfully erase all configuration info from flash。
```

提示：

该命令只擦除本机的启动配置信息，而 hlink 配置信息完成对所管理设备的系统设置，不会被擦除。如果想要擦除 h.link 的配置只能在 hlink-root 节点下执行该命令。

2.2.14 exit

【命令作用】退出当前模式，返回上一模式

【命令语法】exit

【命令模式】只读模式和配置模式

【使用指导】在普通用户模式下执行此命令，系统将退出 HammerOS 系统，与 quit 和 logout 效果一样。在配置模式下执行此命令将退回到只读模式。

【配置实例】

使用 exit 命令 (普通用户模式)

Harbour> exit

Exit.

Disconnected.

```
Thanks for using Harbour Networks's product.
Bye!


##########################################################
#                                                        #
#                 Welcome to HammerOS.                   #
#                                                        #
#      Press Return to connect and config this system.   #
#                                                        #
##########################################################
```

使用 exit 命令 (管理员配置模式)

Harbour(config)# exit

Harbour>

【相关命令】quit,logout

2.2.15 常用命令列表

表 2-4 列出了只读模式下的常用命令。

表 2-4：只读模式下的常用命令

命令	描述
clear	清除屏幕信息
enable	进入配置模式，可以对交换机进行配置和写操作
exit	退出当前配置模式，返回到上一级配置模式
help	显示如何使用命令行中的语法帮助
list	显示当前可用的命令列表
logout	退出登录，断开连接
quit	退出命令行，断开连接（这个命令跟 logout 作用相同）
show history	显示已输入的历史命令
show service	显示当前系统提供的服务
show idle-timeout	显示 idle timeout（空闲超时）时间

show version	显示 HammerOS 的版本信息
show time	显示系统日期
show modem [<modemlist>|all]	显示 Modem 端口信息
terminal length <0-512>	设置终端每屏输出的行数
telnet <A.B.C.D>	使用 Telnet 连接到另一交换机
who	显示当前连接到交换机的用户

只读模式下除了 enable 以外的所有命令在配置模式下都有效，所以在表 2-5 列出配置模式下常用命令时就不再重复这些命令，配置模式下常用命令比较多，具体见附录。

表 2-5：配置模式下的常用命令

命令	描述
enable-password	修改自己进入配置模式的密码
config time <1970-2100> <1-12> <1-31> <HH:MM:SS>	修改日期时间，依次为年、月、日、时、分、秒
erase {startup-config}*1	删除交换机中保存的系统启动配置信息
hostname <hostname>	给交换机重新起个名字，在本文档中，交换机的缺省名字为 Harbour
idle-timeout <0-35791>	设置经过多长的空闲等待时间，系统自动进入登录前的状态，单位是分钟，设置为 0 表示总是处于连接状态
config webbrowser fresh-interval <second>	配置 Web 浏览器的刷新时间间隔
show running-config	显示系统当前正在运行的配置
show startup-config	显示系统的启动配置
config syscontact <.contact>	描述主机管理员的信息，包括用户名、联系方式等（根据需要来设定）
config syslocation <.location>	描述主机的位置
show syscontact	显示管理本主机的用户，以及如何联系该用户
show syslocation	显示主机所在的物理位置
save {configuration}*1	把当前正在运行的配置写到交换机中并保存

注意：

HammerOS 的命令行的所有命令都是不区分大小写的。

2.3 设置用户访问权限

HammerOS 中提供了两种用户权限：

- ADMIN 管理员
- NORMAL普通用户

普通用户登录到 HammerOS 系统后，只能进入只读模式而不能进入配置模式。普通用户能查看大部分系统信息，只有以下信息对普通用户是不可见的：

- 系统中的用户信息
- 系统的配置信息（主要指系统中的配置文件内容以及系统全局配置信息）

管理员能进入配置模式并对系统的所有参数进行查看和设置。系统管理员还能增加、删除用户帐号，设置修改用户密码，修改用户权限，以及进行系统全局信息的配置等。

2.3.1 系统缺省用户帐号

系统缺省内置了一个用户帐号，用户名是 admin，缺省密码是 harbour。用户是管理员。缺省用户 admin 的帐号不能被删除，用户名也不能被修改，只能修改它的密码。

2.3.2 增加用户帐号

可以按照以下步骤建立用户帐号：

1. 以用户名 admin 登录（或者用任何其他管理员的用户帐号登录）；
2. 输入密码，进入只读模式；
3. 在只读模式下，输入 enable 命令，输入配置模式密码，进入配置模式；
4. 在配置模式下，输入以下命令创建一个用户帐号：

【命令语法】`user add <username> login-password <login_password>`

【参数说明】

参数	说明
username	所要添加用户的名称，用户名必须为以字母开头的，只包含大写或小写英文字母、数字、下划线的长度为 4-20 的字符串。
login_password	该用户的登录密码，可以是由任意字符组成的长度为 6-20 的字符串。

注意：

系统对于用户名是不区分大小写的，对密码区分大小写。

通过上述方法创建的用户一般都是普通用户，如果想要创建一个管理员的用户帐号，可以在按照以上步骤创建完用户帐号后，对用户权限进行修改。具体见本章下一节（修改用户权限）

【配置实例】增加一个用户，用户名为 manager

在配置模式下，键入命令：

Harbour(config)# user add manager login-password harbour

按回车，显示如下信息：

Successfully added user manager as a NORMAL_USER ,

To change user role use "user role" command 。

表明用户已经成功添加。

2.3.3 修改用户权限

由于本系统中有两个不同级别的用户，所以通过以下两条命令可以将管理员用户转变为普通用户，也可以将普通用户转变为管理员用户。

- 将一个用户设为管理员，使用命令：

【命令语法】 user role <username> ADMIN enable-password <enable_password>

【参数说明】

参数	说明
username	用户的用户名
enable_password	用户的登录密码

- 将管理员设为普通用户，使用命令：

【命令语法】user role <username> NORMAL

【参数说明】

参数	说明
username	管理员的用户名

【配置实例】将添加的用户 manager 的权限改为系统管理员

在配置模式下，键入命令：

Harbour(config)# user role manager admin enable-password harbour

按回车，显示如下信息：

Successfully change user manager to ADMIN mode。

表明用户权限已经成功修改。

2.3.4 查看系统用户信息

查看用户列表。

【命令语法】`user list`

【配置实例】在配置模式下，键入命令：

Harbour(config)# user list

按回车，显示如下信息：

UserName --------------- User_role ----------

admin ADMIN_USER

manager NORMAL_USER

Total 2 users in system。

2.3.5 删除用户帐号

可以用以下命令删除一个用户帐号：

【命令语法】`user delete <username>`

【参数说明】

参数	说明
username	用户名

2.3.6 修改密码

管理员修改自己的登录密码，在配置模式下输入：

Harbour(config)# login-password

根据提示，输入新密码和确认新密码即可。管理员除了能够修改自己的登录密码外，还能修改自己进入配置模式的密码，可以用以下命令修改自己进入配置模式的密码：

在配置模式下输入：

Harbour(config)# enable-password

然后在提示符下输入新密码和确认新密码即可。

此外，管理员还能够重新设置其他用户的密码，用以下命令：

【命令语法】user login-password <username>

user enable-password <username>

【参数说明】

参数	说明
username	用户名

【使用指导】在提示符下输入新密码和确认新密码，就可以设置用户的登录密码和配置模式密码。

【配置实例】

修改用户 manager 的登录密码为 network，键入命令：

Harbour(config)#user login-password manager

按回车，执行该命令。并输入新密码：network 和确认新密码：network。

修改用户 manager 进入配置模式的密码为 enter_config，键入命令：

Harbour(config)# user enable-password manager

按回车，执行该命令。并输入新密码：enter_config 和确认新密码：enter_config

注意：

执行该命令必须确保 manager 是 admin 用户，否则系统会报错！

2.4 管理 Hammer3100 系列交换机的途径

Hammer3100 系列交换机主要有以下几个管理途径：

- 使用一个终端（或者仿终端软件）连接到交换机的串口（Console），从而通过终端来访问交换机的命令行接口（CLI）。
- 使用Telnet管理交换机。
- 使用SNMP管理软件管理交换机。
- 使用Web浏览器如Internet Explorer来管理交换机。

本交换机同时能支持多个连接：

- 1个Console口连接
- 最多同时能支持4个Telnet连接
- 最多同时能支持4个用户连接
- 1个用户最多同时开2个连接

2.4.1 使用 Console 口连接到交换机

可以通过在交换机前面板上标有“ CONSOLE ”字样的 RJ-45 串口访问交换机内置的命令行接口。连接到 Console 端口的终端应按如下配置：

波 特 率	：	9600
数 据 位	：	8
奇偶校验	：	无
停 止 位	：	1
流量控制	：	无

在使用 Console 口连接交换机时，推荐用户使用 VT100 终端仿真。设置方法：在超级终端界面中，打开“ **文件** ”菜单，选择“ **属性** ”工具条，出现一个窗口，点击“ **设置** ”标签，在终端仿真下拉列表中选择 VT100 即可。如下图所示：

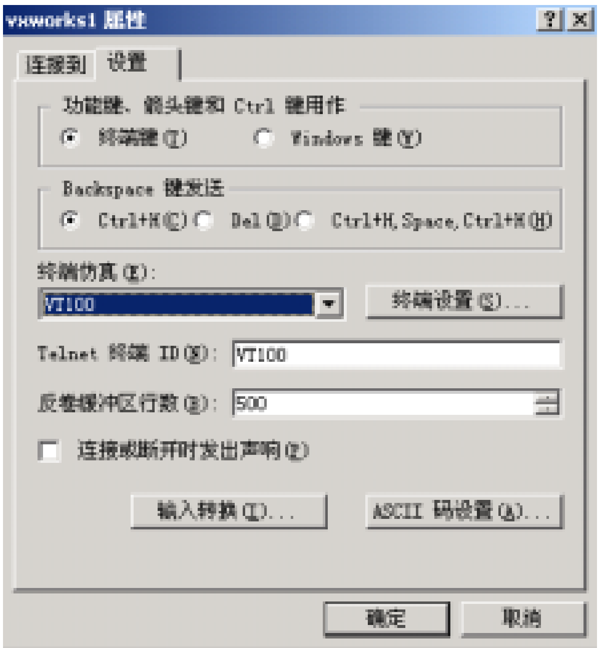


图 2-1

如果连接成功，在终端中看到操作系统启动的界面后，您就可以通过命令行接口对交换机进行配置了。

【例如】通过 Console 口连接登录到交换机后，我们给交换机配置一个 192.168.0.232 的 IP 地址

第一步：将交换机的 Console 口和特定终端连接起来，正常给交换机供电。

第二步：待 HammerOS 成功启动后，就可以看到交换机的提示登录信息：

```
##############################################################
#                                                            #
#                  Welcome to HammerOS.                      #
#                                                            #
#         Press Return to connect and config this system.    #
#                                                            #
##############################################################
```

按回车键进行登录。

第三步：此时，系统要求您输入用户名和密码。

1. 如果您是首次登录交换机，您就应该使用缺省的用户名 admin，来进行登录，此时输入登录密码 harbour，按回车键，进入只读模式，输入 enable，按回车，键入配置模式缺省密码 harbour。
2. 如果您已经分配了一个自己的用户名和密码，而且您已有系统管理员的权限，那么，登录时就使用自己的用户名和密码。

第四步：当您成功登录交换机时，系统显示如下信息：

Habour(config)#

表明您可以对命令行进行操作了。

第五步：然后给交换机配置 IP 地址。输入命令：

Harbour(config)# config ipaddress 192.168.0.232/24

成功执行该命令后，就可以从该 VLAN 的端口上以该 VLAN 的 IP 地址 Telnet 登录到交换机的命令行接口。

第六步：保存配置，键入命令：

Harbour(config)# save configuration

按回车，当出现如下提示信息时：

Trying save configuration to flash, please wait ......

Preparing configuration data to save...Done。

Starting write configuration data to flash...Done。

Configuration save to flash successfully。

表明系统向 Flash 中写入配置信息成功，即保存成功。

而且所做的配置立即生效。

第七步：当您完成对交换机的操作后，键入命令：logout 或 exit

就可以断开与交换机的连接，并退出命令行界面。

2.4.2 使用 Telnet 管理交换机

任何一个有 Telnet 功能的工作站都能通过 TCP/IP 网络连接到交换机，从而实现对交换机的配置管理。如果使用 Telnet 登录交换机，首先应该给交换机配置一个 IP 地址。

然后在配置模式下输入如下命令：

【命令语法】telnet <A.B.C.D>

【参数说明】

参数	说明
A.B.C.D	交换机 IP 地址

注意：

这里的 Telnet 工作站的 IP 地址与本交换机的 IP 地址应该在同一网段。

【配置实例】远程登录一台 IP 地址为 192.168.0.232 的交换机，在配置模式下，键入命令：

Harbour(config)# telnet 192.168.0.232

按回车，出现信息：

Trying 192.168.0.232...

Press Ctrl-Q to abort connect.

Connected to 192.168.0.232.

Press Ctrl-Q to force exit telnet.

HammerOS Release Version1.2 on MicroHammer VDSL Switch.

Login:

输入用户名和密码进行登录。

Hammer3100 系列交换机提供利用 Telnet 功能管理交换机，这样远程用户就可以通过网络控制和管理远端的交换机，给用户和网管员提供了方便，但是这样就存在了安全隐患，为了防止非法用户对交换机的控制，在 Hammer3100 系列交换机上提供了相应的 Telnet 安全策略：我们可以创建一系列 Telnet 规则，只有那些匹配网段上的主机才可以利用 Telnet 登录到 Hammer3100 系列交换机，这样就极大的增加了 Telnet 的安全性。

1) 创建一条 Telnet 规则

【命令语法】`create ipfilter ipaddress <A.B.C.D/M> [permit|deny]`

create ipfilter ipaddress <A.B.C.D> <A.B.C.D> [permit|deny]

【参数说明】

参数	说明
<A.B.C.D/M>和<A.B.C.D/A.B.C.D>	这两种形式可以任选其一,第一种形式中的/M 代表子网掩码的长度，M 的取值范围是 1-32。第二种形式的子网掩码是点分十进制形式。
permit	允许来自 <A.B.C.D/A.B.C.D>网段的 Telnet 包通过。
deny	禁止来自<A.B.C.D/A.B.C.D>网段的 Telnet 包通过。

【使用指导】Hammer3100 系列交换机对存在包含关系的网段按掩码的长度从大到小排列。即匹配规则时首先匹配掩码长的网段。这样就可使网络管理人员灵活的调整 Telnet 管理策略。

【配置实例】网管先是执行命令：

Harbour(config)# create ipfilter ipaddress 192.168.0.0/16 permit

该命令允许 192.168.0.0/16 网段的主机都可 Telnet 登录交换机。但是后来网管认为，该网段的部分主机不允许 Telnet 登录到交换机。于是又设置如下：表示允许 192.168 网段上除了 192.168.0.23/32 和 192.168.0.24/32 这两台主机之外的工作站都可以通过 Telnet 登录到交换机。

Harbour(config)# create ipfilter ipaddress 192.168.0.23/32 deny

Harbour(config)# create ipfilter ipaddress 192.168.0.24/32 deny

2) 配置非匹配规则下的 Telnet 包的处理方式

【命令语法】`config ipdefrule [permit|deny]`

【参数说明】

参数	说明

permit	允许在非匹配规则下的 Telnet 数据包登录到交换机
deny	禁止在非匹配规则下的 Telnet 数据包登录到交换机

【配置实例】

Harbour(config)#config ipdefrule permit

3) 使能或者禁用 Telnet 过滤规则

【命令语法】config ipfilter [enable|disable]

【参数说明】

参数	说明
enable	使能 Telnet 过滤规则
disable	禁止 Telnet 过滤规则

【使用指导】创建 Telnet 规则后一定用 config ipfilter 命令才可以使这条 Telnet 规则生效。

【配置实例】

Harbour(config)#config ipfilter enable

4) 查看 Telnet 规则

【命令语法】show ipfilter

【使用指导】可以利用该命令查看交换机当前的 Telnet 规则。

5)使能或者禁用 Telnet 服务

【命令语法】service telnet [enable|disable]

【参数说明】

参数	说明
enable	使能 Telnet 服务
disable	禁用 Telnet 服务

【使用指导】 可以用 show services 命令查看系统提供的 Telnet 服务是否被使能：如果显示 Service telnet is up 则表明 Telnet 已经使能 如果显示 Service telnet is down 则表明 Telnet 已经禁用。

6)强制禁用一个非法 Telnet 连接

【命令语法】kill session <1-24>

【参数说明】

参数	说明
<1-24>	sessionId 的取值范围

【使用指导】具有管理员权限的用户可以强制断开一个 Telnet 连接。用 who 命令查看当前连接的用户，如果发现有一个用户连接是非法的，那么可以根据用 who 命令所看到的该连接的 sessionId，然后再用该命令强制断开那个连接。如果您输入的 session 是 Console 口连接的，将出现以下提示信息：

```
You can't kill a console session。
```

通过这种方法可以防止非法用户的登录，提高系统的安全特性。

2.4.3 配置 SNMP

简单网络管理协议 SNMP（Simple Network Management Protocol）提供了一种监控和管理计算机网络系统的方法。当网络管理者利用 SNMP 来管理交换机时，要求在管理平台上建立 Management Information Base（MIB 管理信息库），使网络中的所有变量都存放在 MIB 数据结构中。

使能或禁用 SNMP 服务

1．使能 SNMP 服务：

【命令语法】 service snmp enable

【配置实例】

```
Harbour(config)# service snmp enable
Successfully changed snmp agent service to up.
```

2．禁用 SNMP 服务：

【命令语法】 service snmp disable

【配置实例】

```
Harbour(config)# service snmp disable
Successfully changed snmp agent service to down.
```

可以用 show service 命令查看系统提供的 SNMP 服务的状态：

- 如果显示Service snmp agent is up，表明SNMP服务已经被使能；
- 如果显示Service snmp agent is down，表明SNMP服务已经禁用。

SNMP 参数配置

【命令语法】 config snmp community [readonly|readwrite] <string>

【参数说明】

参数	说明
readonly	读确认 Community 字符串，允许对交换机进行只读访问，缺省值为 public。
readwrite	读写确认 Community 字符串，提供了对交换机读写操作的权限，缺省值为 private。
string	Community 字符串

【使用指导】 Community 字符串为远程网络管理员配置交换机提供了一种用户确认机制。在交换机上有两种 Community 字符串，如上参数说明所述。

【命令模式】 配置模式

【相关命令】 show snmp community-string

该命令可用于查看 SNMP 的 Community 字符串信息。

打开或关闭代理发送 Trap 报文功能

【命令语法】 service snmp trap [enable|disable]

【参数说明】

参数	说明
enable	使能代理发送 Trap 报文功能
disable	禁用代理发送 Trap 报文功能

【命令模式】 配置模式

添加 Trap Receiver

【命令语法】 config snmp trapreceiver add <A.B.C.D> version [v1|v2c] {community <string>}*1

【参数说明】

参数	说明
trapreceiver	接收 Trap 信息的主机
<A.B.C.D>	Traprceiver 的 IP 地址
v1/v2c	表示 Trap 两个版本

{community <string>}*1	如果这个 Traprceiver 同时还承担对交换机的远程配置，那么可以为其设置 Community 字符串。

【命令模式】 配置模式

【配置实例】 添加一个 Trap Receiver，地址为 10.1.30.100，Trap 的版本是 v1，键入命令：

```
Harbour(config)#config snmp trapreceiver add 10.1.30.100 version v1
Successfully added trapreceiver IP address is 10.1.30.100
The trap version is v1
The default trap community is public
```

删除 Trap Receiver

【命令语法】 config snmp trapreceiver delete <A.B.C.D>

【参数说明】

参数	说明
<A.B.C.D>	Trap Receiver 的 IP 地址

【命令模式】 配置模式

【配置实例】 删除一个地址为 10.1.20.20 的 Trap Receiver。

Harbour(config)# config snmp trapreceiver delete 10.1.20.20

显示 Trap Receiver 信息

【命令语法】 show snmp trapreceiver

【命令模式】 配置模式

【配置实例】 显示 SNMP 的 Trap Receiver 信息。

```
Harbour(config)# show snmp trapreceiver
IP address              Version          Community
10.1.30.100             v1                 public
Total 1 trapreceiver IP address in system.
```

2.4.4 使用 Web 浏览器管理交换机

HammerOS 是一个运行在交换机上的可以对设备进行管理的操作系统，任何一个有 Web 浏览

功能的工作站都能通过 TCP/IP 网络连接到交换机，并通过 Web 来实现对交换机的管理。通过 Web 浏览器登录到交换机的具体步骤如下：

- 同Telnet 一样，需要给交换机配置一个IP地址。
- 将交换机的Web功能使能。
- 通过网线将工作站与交换机的一个端口连接起来。
- 然后打开Web浏览器如Internet Explorer，在地址栏中输入所配置的IP地址值。
- 看到登录界面后输入用户名和密码，就可进入配置界面。

提示：

有关 Web 浏览器管理交换机的详细内容见本文档第 11 章。

使能或者禁用 Web 服务，利用命令：

【命令语法】`service webserver [enable|disable]`

【参数说明】

参数	说明
enable	表示使能 Web 服务功能
disable	表示禁用 Web 服务功能

可以用 show service 命令查看系统提供的 Web 服务状态

- 如果显示Service Web manage is up，表明Web服务已经被使能；
- 如果显示Service Web manage is down，表明Web服务已经禁用。

2.5 存取配置文件

在每次对交换机的配置进行修改后，都要对所做的修改进行保存。键入命令

```
Harbour(config)# save configuration
```

将修改后的配置保存到交换机的扩展 Flash 中。当显示如下提示信息时：

```
Configuration save to flash successfully。
```

表明保存配置已经成功。

用户还可以把一份好的配置文件保存到文本文件中，在需要的时候（例如不小心把交换机配置搞乱了，不知道怎样把配置恢复到以前的状态时）再把配置文件下载到交换机中。下载可以有

2 种方法，可以用 FTP 下载，也可用 Xmodem 下载。

此外，用户可以将交换机中的配置文件内容上传到本地磁盘文件中，上传可以有 2 种方法，可以用 FTP 上传，也可用 Xmodem 上传。

2.5.1 通过 FTP 协议下载文件

【命令语法】 download ftp [hammeros|config-file] <A.B.C.D> <username> <password> <filename>

【参数说明】

参数	说明
hammeros	下载文件为系统应用程序文件
config-file	下载文件为系统配置信息文件
<A.B.C.D>	FTP 服务器的 IP 地址
<username>	FTP 服务器的用户名
<password>	FTP 服务器的密码
<filename>	所生成的文件名

【使用指导】通过 FTP 协议下载文件即把主机上的配置文件、系统应用程序文件下载到交换机 Flash 中的过程，可以利用该命令。

【配置实例】假设地址 10.1.30.16 处存在一 FTP 服务器，并且此服务器上存在一个名为 sysconfig.txt 的配置文件，用户 userA 为此服务器的合法用户，密码是 harbour，在配置模式下，输入命令：

Harbour(config)# download ftp config-file 10.1.30.16 userA harbour sysconfig.txt

系统显示如下信息：

Trying download file from ftp server, please wait...

Successfully finished receiving file。

Trying write file to flash......

Finished。

You've successfully download new config file

Now you can type reboot command to reboot system

2.5.2 通过使用 Xmodem 协议下载文件

【命令语法】 download xmodem [hammeros|config-file]

【参数说明】

参数	说明
hammeros	下载文件为系统应用程序文件
config-file	下载文件为系统配置信息文件

【配置实例】假设你机器上的 c :\windows\desktop 目录下存在一个系统配置文件 :sysconfig.txt，把它下载到你的交换机，可以如下操作：

第一步：在配置模式下输入命令

Harbour(config)#dowload xmodem config-file

Trying download file from console, please wait...

Trying receive file from console use xmodem protocol......

CCC

第二步：打开串口超级终端的 " **发送** " 文件菜单

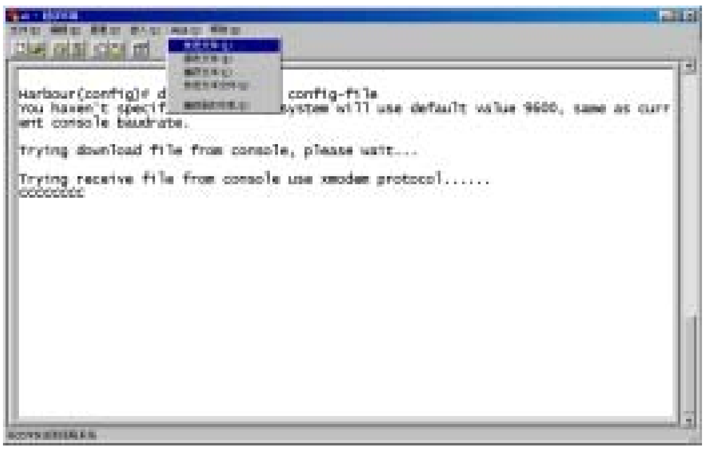


图 2-2

选择您所要下载的配置文件及协议（一定用 Xmodem）

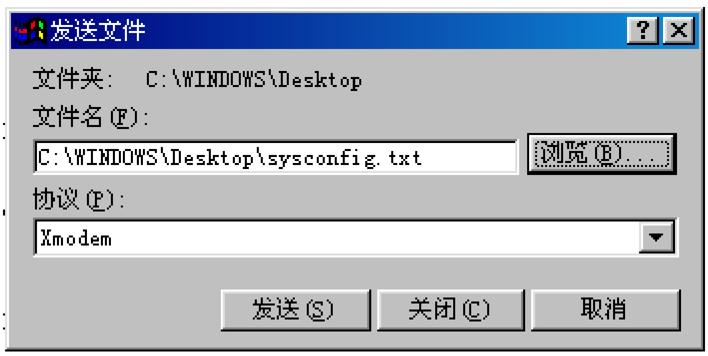


图 2-3

选择“ **发送** ”，系统开始下载指定文件信息。



图 2-4

等待下载完毕后，显示下面信息，表明下载成功，

Successfully finished receiving file。

Trying write file to flash......Finished。

You've successfully download new config file

Now you can type reboot command to reboot system

输入 reboot 命令重新启动交换机。

Writing configuration to flash, please wait ...... finished。

Configuration saved to flash successfully。

2.5.3 通过 FTP 协议上传文件

【命令语法】upload ftp [hammeros|config-file] <A.B.C.D> <username> <password> <filename>

【参数说明】

参数	说明
hammeros	上传文件为系统应用程序文件
config-file	上传文件为系统配置信息文件
<A.B.C.D>	FTP 服务器的 IP 地址

<username>	FTP 服务器的用户名
<password>	FTP 服务器的密码
<filename>	所生成的文件名

【配置实例】假设地址 10.1.30.16 处存在一 FTP 服务器，并且此服务器上存在一个名为 sysconfig.txt 的空白文件，用户 useA 为此服务器的合法用户，密码是 harbour，并具有上传文件的写权限。在配置模式下，输入命令：

Harbour(config)#upload ftp config-file 10.1.30.16 useA harbour sysconfig.txt

系统显示如下信息

Trying upload file to ftp server, please wait...

Successfully finished Upload file。

Finished。

You've successfully upload config file。

表明当前交换机的配置信息已被上传到 FTP 服务器指定目录下

2.5.4 通过使用 Xmodem 协议上传文件

【命令语法】upload xmodem [hammeros|config-file]

【参数说明】

参数	说明
hammeros	上传文件为系统应用程序文件
config-file	上传文件为系统配置信息文件

【配置实例】将系统应用程序文件上传到本地磁盘文件中，按以下步骤进行：

第一步：在配置模式下，键入命令：

Harbour(config)# upload xmodem hammeros

按回车，显示如下信息：

Trying upload file by console, please wait...

Trying upload file by console via xmodem protocol......

Waiting receiver...

第二步：在超级终端中，选择传送菜单的“**接收文件**”

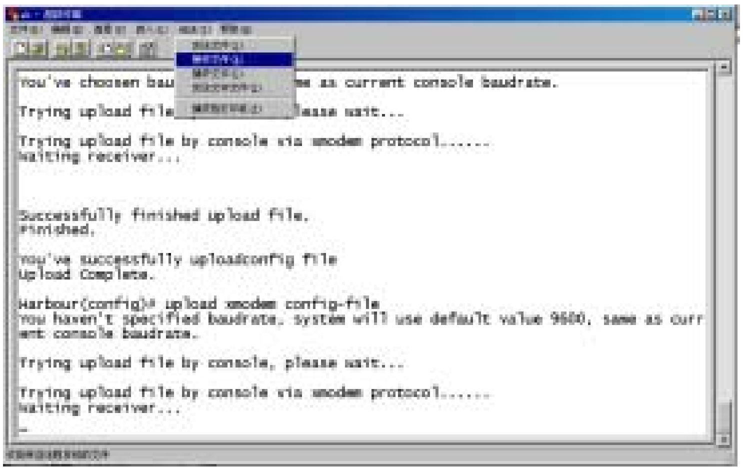


图 2-5

选择存放系统应用程序文件所在的目录，使用的接收协议是 Xmodem，



图 2-6

点击“**接收**”按钮，并输入系统应用程序文件名称，例如：hammeros.bin

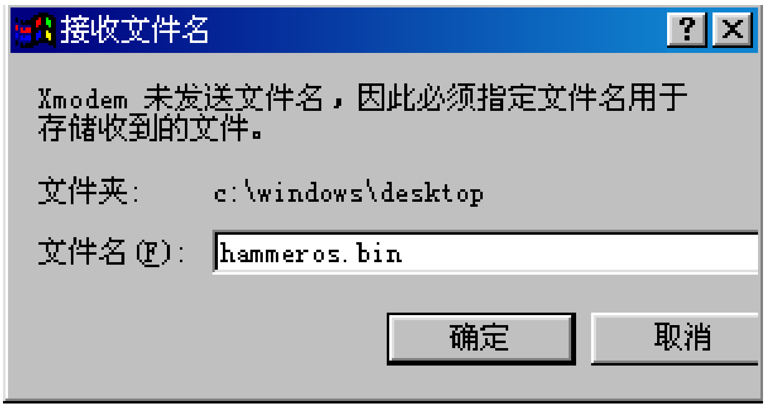


图 2-7

点击“**确定**”按钮出现界面如下：

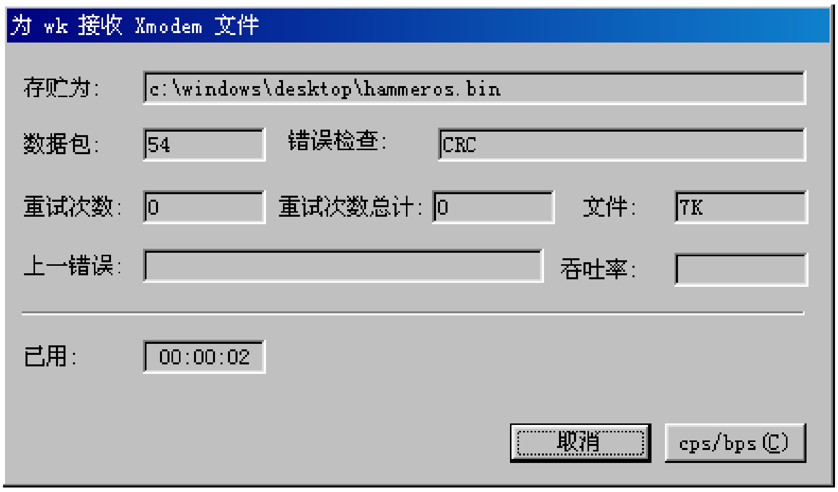


图 2-8

文件上传完毕出现如下提示信息：

Successfully finished upload file。

Finished。

You've successfully uploadimage file

Upload Complete。

到此为止，配置信息上传完毕。

提示：

通过文件的上传和下载，可以很方便的对多台相同配置的交换机进行配置。

2.6 ARP 管理

地址转换协议 ARP（Address Resolution Protocol）提供了主机的 MAC 地址与 IP 地址的映射。交换机会自动学习这种映射并维护映射表。如果对某些特定的主机，您不希望交换机通过自学习的方式获得它们的地址映射，因为在一个庞大的网络中这种学习可能需要占用一定的时间，同时也有学习不到的危险，您也可以通过手工的方式为这些主机建立静态的地址映射表项。

2.6.1 建立静态地址映射表项

【命令语法】 config arp add <A.B.C.D> <mac_address>

【参数说明】

参数	说明
<A.B.C.D>	所连接的某个指定主机的 IP 地址
<mac_address>	所连接主机的物理 MAC 地址

【命令模式】 配置模式

【配置实例】 为某个主机建立一条静态的地址映射表项，该主机的 IP 地址为 10.1.31.41 物理 MAC 地址为 00:50:ba:f2:4b:0a。

Harbour(config)# config arp add 10.1.31.41 0050baf24b0a

2.6.2 删除地址映射表项

【命令语法】 config arp delete [<A.B.C.D>|all]

【参数说明】

参数	说明
<A.B.C.D>	所连接的某个指定主机的 IP 地址，选择这个参数表示要删除该主机的地址映射表项。
all	选择 all 表示删除所有连接的主机的地址映射表项

【命令模式】 配置模式

【配置实例】 删除 IP 地址为 10.1.31.41 的主机的地址映射表项。

Harbour(config)# config arp delete 10.1.31.41

2.6.3 显示地址映射表项

【命令语法】 show arp {[<A.B.C.D>|permanent]}*1

【参数说明】

参数	说明
<A.B.C.D>	IP 地址所对应主机的地址映射表项
permanent	所有的静态地址映射表项

【使用指导】 如果不输入任何参数，则显示包括动态和静态映射地址表项在内的所有映射地址表项。

【命令模式】 只读模式和配置模式

【配置实例】 显示所有的映射地址表项。

```
Harbour(config)# show arp
Arp table information

Physics Address     Ip Address          Type
```

```
----------------  ------------------  ---------
00:10:5c:b4:49:6f  10.1.30.80        dynamic
00:50:ba:f2:4b:0a  10.1.31.41        permanent
----------------  ------------------  ---------
```

Total 2 information

2.7 配置交换机的 IP 地址

由于本设备是二层交换机，只能配置一个 IP 地址（也即缺省网关），配置 IP 地址的方法如下：

【命令语法】 config ipaddress <A.B.C.D/M> 或者

config ipaddress <A.B.C.D > <A.B.C.D >

【参数说明】

参数	说明
<A.B.C.D/M> <A.B.C.D > <A.B.C.D >	交换机配置的 IP 地址，M 表示子网掩码长度，或者按照第二种命令语法格式将 M 改写成 IP 的形式

【命令模式】 配置模式

【配置实例】 将交换机的 IP 地址配置为 192.168.0.232，子网掩码为 255.255.255.0。

Harbour(config)# config ipaddress 192.168.0.232 255.255.255.0

或者键入命令：

Harbour(config)# config ipaddress 192.168.0.232/24

利用 show ip 命令可以查看交换机的 IP 地址，例如：

```
Harbour(config)# show ip

Switch ip address information:

-----------------------------------
Switch ip address  : 192.168.0.232
Switch netmask     : 255.255.255.0
-----------------------------------
```

2.8 配置静态路由

静态路由是由用户定义的一条可使数据包从源地址通过指定路径到达目的地址的路由。当动态路由协议未能创建一条到特定目的的路由时，静态路由就显得尤为重要。还可以通过配置某一静态路由为默认路由，把无路由的数据包发送到默认的网关。

2.8.1 增加静态路由

【命令语法】ip route <A.B.C.D/M> <A.B.C.D>

ip route <A.B.C.D > <A.B.C.D> <A.B.C.D>

【参数说明】

参数	说明
<A.B.C.D/M> <A.B.C.D > <A.B.C.D>	目的网段的 IP 地址和子网掩码长度，或者按照第二种命令格式将子网掩码由长度 M 的形式改为 IP 地址的形式
<A.B.C.D>	最后一个参数<A.B.C.D>为下一跳的 IP 地址

【使用指导】注意：这里的 IP 地址应该与本交换机的 IP 地址在同一个网段。

【配置实例】在交换机上进行如下配置：

Harbour(config)#config ip 10.1.2.3/8

Harbour(config)#ip route 169.254.1.1/24 10.1.2.5

2.8.2 删除静态路由

【命令语法】 no ip route <A.B.C.D/M> <A.B.C.D>

no ip route <A.B.C.D> <A.B.C.D> <A.B.C.D>

【参数说明】

参数	说明
<A.B.C.D/M> <A.B.C.D> <A.B.C.D>	目的网段的 IP 地址和子网掩码长度，或者按照第二种命令格式将子网掩码由长度 M 的形式改为 IP 地址的形式
<A.B.C.D>	最后一个参数<A.B.C.D>为下一跳的 IP 地址

【使用指导】注意：这里的 IP 地址应该与本交换机的 IP 地址在同一个网段。

2.8.3 显示静态路由信息：

【命令语法】 show ip route

【使用指导】 显示的内容包括目标 IP 地址、子网掩码和下一跳网关的 IP 地址。

【命令模式】 只读模式和配置模式

【配置实例】

```
Harbour(config)# show ip route
***    begin route table info ***
Destination net-----NetMask-------------Gateway-------------
10.0.0.0          255.0.0.0            10.1.2.3
127.0.0.1         255.255.255.255      127.0.0.1
169.254.1.0       255.255.255.0        10.1.2.5
***    end route table info ***
```

2.9 ACL（Access Control List）访问控制列表的配置

本节主要包括以下内容：

- 访问控制模块概述
- 打开/关闭访问控制服务
- 添加/删除访问控制列表表项
- 配置缺省规则
- 查看访问列表表项

2.9.1 访问控制功能概述

访问控制模块主要是为了提高系统的安全性。通常情况下，只要用户拥有登录名和密码就可以登录到交换机，但有时我们出于安全性的考虑，希望用户的IP地址是某个特定值或者是一个范围网段，这时就可以打开控制访问服务，将IP地址加入到访问配置表。当用户登录时，交换机首先验证该用户IP地址的合法性，如果IP合法，才会验证用户名和密码的合法性。

系统最多允许创建20个访问控制配置表项。

2.9.2 打开/关闭访问控制服务

【命令语法】 `config ipfilter [enable|disable]`

【参数说明】

参数	说明
enable	打开访问控制服务
disable	关闭访问控制服务

【命令模式】配置模式

2.9.3 添加/删除访问控制列表表项

添加访问控制列表表项

【命令语法】create ipfilter ipaddress <A.B.C.D/M> [permit|deny]

create ipfilter ipaddress <A.B.C.D> <A.B.C.D> [permit|deny]

【参数说明】

参数	说明
<A.B.C.D/M> <A.B.C.D/A.B.C.D>	网段的 IP 地址和子网掩码长度，或者按照第二种命令格式将子网掩码由长度 M 的形式改为 IP 地址的形式
permit	把指定的 IP 表项设置成允许访问
deny	把指定的 IP 表项设置成拒绝访问

【命令模式】配置模式

【配置实例】

Harbour(config)#creat ipfilter ip 192.168.0.200 255.255.255.0 permit

删除访问控制列表表项

【命令语法】delete ipfilter all

delete ipfilter ipaddress <A.B.C.D/M>

delete ipfilter ipaddress <A.B.C.D> <A.B.C.D>

【命令模式】配置模式

【配置实例】

Harbour(config)#delete ipfilter 192.168.0.88/16

2.9.4 配置缺省规则

【命令语法】 config ipdefrule [permit|deny]

【使用指导】 把 IP 不在已经添加到配置列表表项范围内的其他 IP，缺省规则配置成允许或拒绝访问。

【命令模式】配置模式

【配置实例】

Harbour(config)#config ipdefrule deny

2.9.5 查看访问列表表项

【命令语法】 show ipfilter

【使用指导】 显示的内容包括各个表项和缺省规则。

【命令模式】 只读模式

【配置实例】

Harbour(config)#show ipfilter

```
---------------------------IP FILTER START-------------------------------
Ipfilter enable
192.168.  0.200   255.255.255.   0          : permit
Default rule                                 : permit

---------------------------IP FILTER END---------------------------------
totle 2    rules
```

2.9.6 访问控制列表的命令列表

命令	描述
config ipdefrule [permit|deny]	配置缺省规则
config ipfilter [enable|disable]	打开/关闭访问控制服务
create ipfilter ipaddress <A.B.C.D/M> [permit|deny] create ipfilter ipaddress <A.B.C.D> <A.B.C.D> [permit|deny]	添加一条访问控制表项
delete ipfilter all delete ipfilter ipaddress <A.B.C.D/M> delete ipfilter ipaddress <A.B.C.D> <A.B.C.D>	删除访问控制表项
show ipfilter	查看访问列表表项

2.10 检测网络的基本连接情况

交换机提供了 ping 命令用来检测网络的基本连接情况：ping 命令发送 Internet Control Message Protocol (ICMP) echo 消息到网络中的某个 IP 设备。普通用户和管理员用户都可以使用 ping 命令。

【命令语法】ping {[-t]}*1 {[-count] <1-65535>}*1 {[-size] <0-6400>}*1 {[-waittime] <1-255>}*1 {[-ttl] <1-255>}*1 {[-pattern] <user_pattern>}*1 <A.B.C.D>

【参数说明】

参数	说明
-t	使用 t 选项后,ping 命令将一直向目标 IP 地址发送 ICMP echo 消息，直到用户用 Ctrl+c 中断。 缺省不用 t 选项时，ping 命令发送完 5 个 ICMP echo 消息就停止发送了。
-count <1-65535>	count 选项指定 ping 程序总共发送多少个 ICMP echo 消息后就退出 ping 程序。
-size <1-6400>	size 选项指定发送的 ICMP echo 消息的附加内容长度。
-waittime <1-255>	waittime 选项指定 ping 程序等待多少秒之后如果还未收到应答就认为目标不可通。
-ttl <1-255>	ttl 选项指定 ICMP 数据包的 ttl（time to live）值。
-pattern <user_patter>	pattern 选项指定 ICMP 数据包中用户自己定义的 1-16 个 16 进制数。

【使用指导】ping 命令的众多选项可以都不输入，而使用最简单的格式。例如：

```
ping 192.168.0.1
```

用来测试交换机是否可以跟 IP 地址为 192.168.0.1 的设备连接通信。

如果设备连通，则出现以下信息：

```
PING 192.168.0.1 : 56 data bytes.
Press Ctrl-c to Stop.
Reply from 192.168.0.1 : bytes=56: icmp_seq=0 ttl=128 time=100 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=1 ttl=128 time=33 ms
Reply from 192.168.0.1 : bytes=56: icmp_seq=2 ttl=128 time=33 ms

----192.168.0.1 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss

round-trip(ms) min/avg/max = 0/36/100
```

如果设备没有连通，出现以下信息：

```
PING 192.168.0.1 : 56 data bytes.
Press Ctrl-c to Stop.
```

```
Request time out.
Request time out.
Request time out.

----192.168.0.1 PING Statistics----
5 packets transmitted, 0 packets received, 100% packet loss
```

2.11 使能/禁用广播抑制功能

交换机提供了广播抑制功能，当广播风暴发生时，交换机会收到大量的广播报文，当收到的广播包的速率达到一定值时，交换机开始抑制广播报文的收发，并丢弃某些广播包，使交换机不至于瘫痪。

【命令语法】config broadcast-limite off

config broadcast-limite on {<10-10230>}*1

【参数说明】

参数	说明
off	禁用广播抑制功能
on	使能广播抑制功能
10-10230	限定的广播包的范围

2.12 关于流控异常的监控功能

由于某种原因，在打开局端流控的时候，某些情况下会导致端口异常发 pause 帧而不能正常通信。打开该监控，能够使这种情况避免。

2.12.1 使能/禁用流控异常的监控功能

【命令语法】config monitor_pause [on|off]

【参数说明】

参数	说明
on	使能流控异常的监控功能
off	禁用流控异常的监控功能

【使用指导】默认为打开监控

【配置实例】禁用流控异常的监控功能。

Harbour(config)#config monitor_pause off

2.12.2 查看流控异常监控的状态

【命令语法】show monitor_pause status

【配置实例】

Harbour(config)#show monitor_pause status

monitor is on

表示当前监控打开。

2.13 系统限制功能

系统限制功能是用于对异常攻击的防范。目前对三种报文（IGMP，STP，IP）做了限制，在一定的时间间隔（大约 0.5 秒）内，用户可以配置各端口最大接收报文的数量，如果在该时间间隔内报文的数量大于用户配置的最大上限，该报文就会被丢弃。缺省的数量：IGMP 为 100 个；IP 为 4294967295 个；STP 为 200 个。

2.13.1 配置系统限制

【命令语法】 config systemlimit [igmp|ip|stp] [all|<portlist>] <0-4294967295>

【参数说明】

参数	说明
[igmp | ip | stp]	数据包的类型
all	所有端口
<portlist>	指定端口
<0-4294967295>	包的最大个数，0 为拒绝所有的包

【配置实例】配置 1 端口的最大 IGMP 类型的数据包为 150 个。

Harbour(config)# config systemlimit igmp 1 150

2.13.2 查看系统限制

【命令语法】show systemlimit [igmp|ip|stp] [all|<portlist>]

参数	说明
[igmp | ip | stp]	数据包的类型
all	所有端口
<portlist>	指定端口

【配置实例】

Harbour(config)# show systemlimit　igmp 1

port　1: permit receiving　　　　150 packet in every interval

2.14 802.1x 报文的扩展

2.14.1 使能、禁止对 802.1x 报文的转发

【命令语法】 `config 802.1x forwarding [enable|disable]`

【参数说明】

参数	说明
enable	使能对 802.1x 报文的转发
disable	禁止对 802.1x 报文的转发

【配置实例】

Harbour(config)# config 802.1x forwarding enable

2.14.2 配置转发 802.1x 报文的出端口

【命令语法】`config port [<portlist>] uplink`

【参数说明】

参数	说明
<portlist>	指定端口

【使用指导】 注意，端口数不能大于 4 并且只有在 802.1x 报文转发使能的情况下，才可以进行配置。

【配置实例】

Harbour(config)# config port 1，4 uplink

2.14.3 查看当前对 802.1x 报文的转发配置

【命令语法】`show 802.1x`

【配置实例】

Harbour(config)# show 802.1x

802.1x forwarding enabled

uplink port list　1,4

2.15 查看当前 CPU 风扇运行情况

在硬件版本为 2.xx 的 Hammer3100 和 Hammer3100-16 上，增加了 CPU 风扇的报警功能，如果出现风扇运行异常，将发出 Trap 和 Syslog。也可以用命令来显示当前风扇运行情况。其它 Hammer3100 上该功能被屏蔽。

【命令语法】`show fan status`

【配置实例】

Harbour(config)# show fan status

warning: CPU fan occurred a fault now!

第3章 配置端口

这一章主要讲述如何使用 HammerOS 来配置交换机的快速以太网端口及 VDSL 端口，主要包括：

- 使能或禁用指定端口
- 使能或禁用指定端口的自适应功能
- 配置端口速度
- 配置端口的半双工或全双工模式
- 配置端口的流量控制
- 配置端口的地址自学习功能
- 配置VDSL端口的自适应功能
- 配置VDSL端口的速率
- 配置VDSL端口的双工模式
- 配置VDSL端口的流量控制
- 配置端口镜像
- 配置多端口负载均衡组
- 端口优先级
- VDSL端口Firmware
- 端口MAC地址限定

3.1 使能或禁用交换机指定的端口

对于启动后的交换机，在缺省情况下，端口都是使能的。当然，您可以根据实际需要对各个端口的状态进行配置。利用以下命令使能或禁用一个或多个指定端口：

【命令语法】config port [<portlist>|all][enable|disable]

【参数说明】

参数	说明
portlist	端口列表，允许一次配置多个端口。
all	表明对所有端口进行操作
enable	使能需要配置的端口
disable	禁用端口

【配置实例】禁用端口 1，3，5，7－12，配置如下：

Harbour(config)#config port 1,3,5,7-12 disable

注意：

此处的端口可以是快速以太网端口。也可以是 VDSL Modem 的端口。

提示：

端口在禁用状态时，出于诊断需要，端口的链路依然是通的。

3.2 配置快速以太网端口

本部分内容所涉及到的快速以太网端口指的是端口 25 和 26；快速以太网端口可以连接 10Base-T 或者 100Base-Tx 网络，可以工作在半双工或全双工模式。这就要求用户根据实际情况对其进行配置。

缺省情况下，Hammer3100 系列交换机的快速以太网端口设置为自适应模式，并根据端口对端的性能自动调整端口的速度和双工模式。用户可以手工配置这些端口的速度、双工和流控模式。要手工配置端口的速度、双工、流控模式，必须禁用端口的自适应模式后再进行配置。

3.2.1 配置快速以太网端口的自适应模式

【命令语法】`config port [<portlist>|all] auto [on|off]`

【参数说明】

参数	说明
portlist	端口列表
all	表示对所有快速以太网端口进行操作
on	使能端口的自适应模式
off	禁用端口的自适应模式

【配置实例】关闭端口 25 的自适应模式。

Harbour(config)# config port 25 auto off

3.2.2 配置快速以太网端口的速度

【命令语法】`config port [<portlist>|all] speed [10|100]`

【参数说明】

参数	说明
portlist	端口列表

all	表示对所有快速以太网端口进行操作
10	把端口的速度设置为 10M 模式
100	把端口的速度设置为 100M 模式

【配置实例】将端口 25 的速度设置为 10Mbps

Harbour(config)# config port 25 speed 10

3.2.3 配置快速以太网端口的双工模式

【命令语法】config port [<portlist>|all] duplex [full|half]

【参数说明】

参数	说明
portlist	端口列表
all	表示对所有快速以太网端口进行操作
full	端口配置为全双工模式
half	端口配置为半双工模式

【配置实例】将端口 25 设置为全双工模式 。

```
Harbour(config)# config port 25 duplex full
```

3.2.4 配置快速以太网端口的流控

【命令语法】config port [<portlist>|all] flowcontrol [on|off]

【参数说明】

参数	说明
portlist	端口列表
all	表示对所有快速以太网端口进行操作
on	使能端口的流量控制功能
off	禁用端口的流量控制功能

【配置实例】使能所有端口的流量控制

```
Harbour(config)# config port all flowcontrol on
```

3.2.5 配置快速以太网端口的学习功能

【命令语法】config port [<portlist>|all] learning [enable|disable]

【参数说明】

参数	说明
portlist	端口列表
all	表示对所有快速以太网端口进行操作
enable	使能端口的学习功能
disable	禁止端口的学习功能

【配置实例】使能端口 25 和 26 的自学习功能

```
Harbour(config)# config port 25,26 learning enable
```

3.2.6 查看端口信息

【命令语法】show port [<portlist>|all] {[configuration|stats]}*1

【参数说明】

参数	说明
portlist	端口列表，可以是交换机上的任意端口。
all	选择所有的端口
configuration	显示端口配置信息
stat	显示端口流量统计信息

【使用指导】缺省不输入任何选项时显示端口配置信息。如果两个参数都不输入，则显示这两个参数所显示的全部信息。

【配置实例】

```
Harbour(config)# show port 1 configuration
--------------------------------------------------------------------------
                 Port:1 's Configuration Information

Link state       : Down          Port state      : Enabled
Learning         : Enable        VlanFiltering   : On

Port Default VID: 2047           Vlan name       : default
Port summary     : normal
--------------------------------------------------------------------------

Harbour(config)# show port 6 stats
-------------------------------------------------------------------
                 Port:6 's Statistics Information
```

```
Total octets          : 30545016
Tx total octets       : 10869        Rx total octets       : 30531631
Tx unicast frames     : 112          Rx unicast frames     : 1612
Tx multicast frames   : 0            Rx multicast frames   : 0
Tx broadcast frames   : 25           Rx broadcast frames   : 447129
Tx pause frames       : 0            Rx pause frames       : 0
Tx under run frames   : 0            Rx unknown frames     : 0
Rx droped frames      : 3720         Rx overflow frames    : 0
CRC error frames      : 37           Oversize frames       : 0
Fragments             : 0            Jabber                : 0
Undersize frames      : 0            length 64 frames      : 811
length 65 frames      : 448025       length 128 frames     : 32
length 256 frames     : 10           length 512 frames     : 0
length 1024 frames    : 0            length 1519 frames    : 0
symbol error          : 0            false carrier         : 0
out discards          : 0            in discards           : 1299
--------------------------------------------------------------------
```

3.2.7 软复位用户端口

由于某种原因，你可能要重新启动用户端口。

【命令语法】 config port [<portlist>|all] reset

【参数说明】

参数	说明
<portlist>	指定端口
all	所有端口

【使用指导】 该命令对端口的整条链路进行软复位，键入此命令后可以看到交换机前面板上相应的 LINK 指示灯灭掉， Modem 前面板的 SYS 同步指示灯也灭掉，Modem 进行复位，复位完成后。指示灯恢复正常。

【配置实例】

Harbour(config)# config port 1 reset

3.3 环路测试命令

【命令语法】test loopback [<portlist>|all] [line]

【参数说明】

参数	说明
portlist	表示可以对多个端口进行环测
all	表示对所有端口进行环测
line	表示对线路进行环测

【使用指导】该命令对用户指定的端口或者所有端口进行远端环测。

【配置实例】

Harbour(config)# test loopback 1 line

Modem 1 loop back OK!

表明线路正常，丢包率是 0。

3.4 配置 VDSL 的端口

本部分内容所涉及到的 VDSL 端口,指的是交换机上连接用户 Modem 的端口。

VDSL 端口可以连接 10Base-T 或者 100Base-Tx 网络，可以工作在半双工或全双工模式。这就要求用户根据实际情况对其进行配置。

缺省情况下，Hammer3100 系列交换机 VDSL 的所有端口设置为自适应模式，流控打开，并根据端口对端的性能自动调整端口的速度和双工模式。用户可以手工配置 VDSL 端口 Modem 方的速率、双工、流控和自学习模式。但必须禁用自适应模式后才可以配置。

3.4.1 配置 VDSL 端口的自适应模式

【命令语法】config modem [<modemlist>|all] auto [on|off]

【参数说明】

参数	说明
modemlist	端口列表
all	表示对所有 VDSL 端口进行操作
on	使能端口的自适应功能
off	禁用端口的自适应功能

【配置实例】禁用端口 1-14 的自适应模式

```
Harbour(config)# config modem 1-14 auto off
```

3.4.2 配置 VDSL 端口速率

【命令语法】 config modem [<modemlist>|all] speed [10|100]

【参数说明】

参数	说明
modemlist	端口列表
all	表示对所有的 VDSL 端口进行操作
10	设置端口速率为 10M
100	设置端口速率为 100M

【配置实例】将端口 12-20 的速率设置为 10Mbps 。

```
Harbour(config)# config modem 12-20 speed 10
```

3.4.3 配置 VDSL 端口的双工模式

【命令语法】config modem [<modemlist>|all] duplex [full|half]

【参数说明】

参数	说明
modemlist	端口列表
all	对所有的 VDSL 端口进行操作
full	将端口设置为全双工工作模式
half	将端口设置为半双工工作模式

【配置实例】将所有的 VDSL 端口都配置为全双工模式。

```
Harbour(config)# config modem all duplex full
```

3.4.4 配置 VDSL 的 Modem 端口的流控

【命令语法】config modem [<modemlist>|all] flowcontrol [on|off]

【参数说明】

参数	说明
modemlist	端口列表
all	表示对所有的连接 Modem 的端口进行操作
on	表示使能流量控制
off	表示禁用流量控制

【配置实例】使能端口 1，3，5，7—14 的流量控制功能。

```
Harbour(config)# config modem 1,3,5,7-14 flowcontrol on
```

3.4.5 配置 VDSL 局端端口流控

【命令语法】config vdsl_port [<portlist>|all] LT_flowcontrol [on|off]

【参数说明】

参数	说明
portlist	端口列表
all	表示对所有的连接 VDSL 的端口进行操作
on	表示使能流量控制
off	表示禁用流量控制

【配置实例】使能端口 1，3，5，7—14 的局端流量控制功能。

```
Harbour(config)# config vdsl_port 1,3,5,7-14 LT_flowcontrol on
```

3.4.6 显示 VDSL 端口信息

【命令语法】show modem [<modemlist>|all]

【参数说明】

参数	说明
modemlist	端口列表
all	表示对所有的 VDSL 端口进行操作

【配置实例】显示 Modem 1 端口的信息，命令如下：

Harbour(config)# show modem 1

如果 Modem 没有同步上，显示如下：

```
---------------------------------------------------------------------------
Port[ 1] vdsl status:
Remote modem connection   : NO
Downstream line rate(mbps): 12.5      Upstream line rate(mbps)  : 12.5
Rt vdsl auto neg          : Enable    Rt ethernet speed         : 100M
Rt ethernet duplex        : Full      Rt ethernet flowctrl      : Enabled
```

如果 Modem 已经同步上，显示如下：

```
---------------------------------------------------------------------------
Port[ 1] vdsl status:
Remote modem connection   : YES       Modem version             : V2.2
Downstream freq(kHz)      : 1831      Upstream freq(kHz)        : 4467
```

```
Downstream Line SNR (dB)   : 43.08    Upstream Line SNR (dB)     : 29.28
Downstream line rate(mbps): 4.17     Upstream line rate(mbps)   : 1.56
Downstream PSD(dBm/Hz)     : -63.72   Upstream PSD(dBm/Hz)       : -119.93
Remote pc connection       : YES      Remote pc pause flowctrl   : Support
Rt vdsl auto neg           : Enable   Rt ethernet speed          : 100M
Rt ethernet duplex         : Full     Rt ethernet flowctrl       : Enabled
```

3.5 配置用户 Modem 的版本号及序列号信息

为了唯一标识 VDSL 的用户，可以对用户 Modem 的版本号及序列号进行配置，配置用户 Modem 的版本号及序列号信息，利用如下命令：

【命令语法】config modem <modemlist> [SERIAL_NO|HARDWARE_VERSION|SOFTWARE_VERSION] <string>

【参数说明】

参数	说明
modemlist	表示用户 Modem 的端口号
SERIAL_NO	配置 Modem 的序列号信息
HARDWARE_VERSION	配置用户 Modem 的硬件版本信息
SOFTWARE_VERSION	配置用户 Modem 的软件版本信息
string	用户配置的字符串

【使用指导】注意，如果选择配置序列号，那么序列号的位数一定是 12 位或者 21 位；硬件版本和软件版本的位数一定是 4 位。如果想查看已经配置的信息，利用命令：

show modem [<modemlist>|all]sysinfo {[SERIAL_NO|HARDWARE_VERSION |SOFTWARE_VERSION]}*1

【配置实例】

Harbour(config)# config modem 21 serial_no 123456789012

Harbour(config)# config modem 21 hardware_version 1.41

Harbour(config)# config modem 21 software_version 2.11

Harbour(config)# show modem 21 sysinfo

Modem 21's serial_no: 123456789012

Modem 21's hardware_version: 1.41

Modem 21's software_version: 2.11

3.6 显示 Modem 版本号及序列号信息

显示用户 Modem 的硬件版本号、序列号、软件版本号的信息，利用如下命令：

【命令语法】show modem [<modemlist>|all] sysinfo {[SERIAL_NO|HARDWARE_VERSION|SOFTWARE_VERSION]}*1

【参数说明】

参数	说明
modemlist	显示指定的用户 Modem 的信息
all	显示所有用户 Modem 的信息
SERIAL_NO	可选，显示用户 Modem 的序列号
HARDWARE_VERSION	可选，显示用户 Modem 的硬件版本信息
SOFTWARE_VERSION	可选，显示用户 Modem 的软件版本信息

【配置实例】显示用户 Modem 21 的信息如下：

Harbour(config)# show modem 21 sysinfo

Modem 21's serial_no: 123456789012

Modem 21's hardware_version: 1.41

Modem 21's software_version: 2.11

提示：

该命令的显示结果不受用户配置的 terminal length 参数限制。

3.7 配置 VDSL 端口的速率等级

一般来说，VDSL 交换机与用户 Modem 间的距离不超过 1500 米，距离越近、线路的质量越好，速率就越快，由于受接入距离及线路质量等条件的影响，还有人为管理上的需要（比如人为控制某一接入用户的速率）就需要对不同的用户 Modem 配置不同的速率等级，要配置 VDSL Modem 的速率等级，利用以下命令：

【命令语法】config modem [<modemlist>|all] [upstream|downstream|both] rate [R16.67|R12.5|R8.33|Rom|R1.04|R4.17|R2.08|R9.38]

【参数说明】

参数	说明
modemlist	Modem 列表

all	表示对所有用户 Modem 进行操作
upstream	表示对上行数据流（从 Modem 到 Switch）的速率进行设定
downstream	表示对下行数据流（从 Switch 到 Modem）的速率进行设定
both	表示对上行和下行速率同时进行设定
R16.67	把数据流速率设定为 16.67Mbps
R12.5	把数据流速率设定为 12.5Mbps
R8.33	把数据流速率设定为 8.33Mbps
Rom	对于指定端口、当为上行数据流时速率为 1.56 Mbps，当为下行数据流时速率为 4.17 Mbps
R1.04	把数据流速率设定为 1.04Mbps
R4.17	把数据流速率设定为 4.17Mbps
R2.08	把数据流速率设定为 2.08Mbps
R9.38	把数据流速率设定为 9.38Mbps

【使用指导】注意，如果交换机上 VDSL 的端口速率设置为 10M，此时用户 Modem 的速率设置最好不要超过 10M。

3.8 软复位用户 Modem

由于某种原因，你可能要重新启动用户 Modem，但是你现在在交换机侧，就需要使用下面的命令：

【命令语法】 config vdsl_port [<portlist>|all] reset

【参数说明】

参数	说明
portlist	表示可以复位多个指定的 Modem
all	表示复位所有的 Modem

【使用指导】本命令可以复位 Modem，键入此命令后可以看到交换机前面板上相应的 LINK 指示灯灭掉， Modem 前面板的 SYS 同步指示灯也灭掉，Modem 进行复位，复位完成后。指示灯恢复正常。

【配置实例】

Harbour(config)# config vdsl_port 21 reset

Reset modem 21 success !

3.9 VDSL 端口 Firmware 相关配置和显示

Firmware（芯片厂家提供的芯片的一些布丁程序）有两个版本，patch50 和 patch56，patch56 的版本比 patch50 要高，在性能上来讲，patch56 更胜一些。用户默认的版本是我们固化在 Modem 里面的，但如果是低级版本，建议升级到高级。

3.9.1 配置 VDSL 端口 Modem 的 Firmware 版本

【命令语法】 config modem [<modemlist>|all] patch50

config modem [<modemlist>|all] patch56

【参数说明】

参数	说明
<modemlist>	Modem 的列表，等同于端口的列表
all	所有的 Modem

3.9.2 配置 VDSL 端口局端的 Firmware 版本

【命令语法】 config switch [<portlist>|all] patch50

config switch [<portlist>|all] patch56

【参数说明】

参数	说明
portlist	表示端口列表，可以对多个端口同时操作
all	表示对所有端口操作

【使用指导】 硬件版本为 2.xx 的 Hammer3100 和 Hammer3100-16 无该命令。

3.9.3 显示 VDSL 端口 Modem 的 Firmware 的版本信息

【命令语法】 show modem [<modemlist>|all] patch-version

【参数说明】

参数	说明
<modemlist>	Modem 的列表，等同于端口的列表
all	所有的 Modem

【配置实例】

Harbour(config)# show modem 1 patch-version

modem 1's patch file ver is 56

3.9.4 显示 VDSL 端口 Switch 的 Firmware 的版本信息

【命令语法】 show switch [<portlist>|all] patch-version

【参数说明】

参数	说明
portlist	表示端口列表，可以对多个端口同时操作
all	表示对所有端口操作

【使用指导】硬件版本为 2.xx 的 Hammer3100 和 Hammer3100-16 无该命令。

【配置实例】

Harbour(config)# show switch 1 patch-version

Port 1's local patch version is 56

3.9.5 配置 VDSL 端口 Modem 的自动升级

我们提供了自动把 patch50 升级为 patch56 的功能，只要用户配置该命令参数为 enable，Modem 就可以进行自动升级，无需再基于端口进行配置

【命令语法】 config auto-update-patch [enable|disable]

【参数说明】

参数	说明
enable	进行自动升级
disable	停止自动升级（缺省）

3.9.6 查看 VDSL 端口 Modem 的自动升级信息

【命令语法】show auto-update-patch

【配置实例】

Harbour(config)# show auto-update-patch

Auto-update-patch is enabled

Status of each port:

not updated: 2 3 4 5 6 7 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

updating: 1

updated: 8

表示自动升级使能，正在升级的是 1 端口 Modem，已经升级完毕的是 8 端口 Modem。

3.10 VDSL 端口的 Modem 的自协商能力设定和查看

在一般的情况下，Modem 的硬件最大自协商能力为 100M 全双工，但是在某些情况下，基于某种需要，需要软件对 Modem 的最大自协商能力进行设定。

3.10.1 根据不同的 Firmware 版本对自协商最大协商能力配置

【命令语法】 `config auto_ability_of_modem [patch50|patch56] [100|10]`

【参数说明】

参数	说明
patch50|patch56	VDSL 端口 Modem 的 Firmware 的版本号
100|10	用户期望设置的 Speed 的最大协商能力

【使用指导】其中 patch50 的 Modem 默认的最大协商能力为 10M, patch56 的 Modem 为 100M。

【配置实例】把所有 patch50 的 Modem 的最大协商能力设置为 100M。

```
Harbour(config)# config auto_ability_of_modem patch50 100m
```

3.10.2 显示不同的 Firmware 版本的 Modem 的当前最大协商能力

【命令语法】`show auto_ability_of_modem [patch50|patch56]`

【配置实例】

Harbour(config)# show auto_ability_of_modem patch50

The max auto-negotiation ability of patch50 is 100m

3.11 VDSL 端口同步机制的配置和查看

3.11.1 同步前的机制（pre-sync-mode）

在 Modem 与交换机同步之前，交换机端有两种模式可以选择，一种是静态模式，一种是动态模式，可以用命令行进行配置。

A.静态模式（Static）：在同步之前，局端的速率参数保持在缺省值（硬件版本为 1.xx 的 Hammer3100 交换机的缺省值是 ROM，硬件版本为 2.xx 的 Hammer3100 交换机和 Hammer3100-16 交换机的缺省值是 12.5）。

B.动态模式（Dynamic）：局端的速率参数在 ROM 和 12.5 之间切换，以便尽快与 Modem 同步。

配置局端速率的同步前模式

【命令语法】 `config pre-sync-mode [<portlist>|all] [static|dynamic]`

【参数说明】

参数	说明
portlist	表示端口列表，可以对多个端口同时操作
all	表示对所有端口操作
static	静态模式
dynamic	动态模式

【使用指导】缺省值为静态模式。

【配置实例】

Harbour(config)# config pre-sync-mode 1 static

查看局端速率的同步前模式

【命令语法】`show pre-sync-mode [<portlist>|all]`

【配置实例】

Harbour(config)# show pre-sync-mode 1

Port 1: pre-sync-mode is dynamic

3.11.2 长线同步失败后的机制(fail-sync-mode)

在某些长线的情况下，如果较高的速率（如 Rate16.7）会导致与该速率同步不上，我们提供了两种模式供用户配置:

A.普通模式（Normal）：在试图同步二次失败后，局端的速率将停止根据 pre-sync-mode 切换，当在某种速率下同步以后，速率将不再调整，然后发个相关 Trap。

B.速率保持模式（rate_keep：在试图同步二次失败后，局端的速率将始终保持在所配置的速率不再做调整，然后发个相关 Trap。

配置局端速率的同步失败后模式

【命令语法】 `config fail-sync-mode [<portlist>|all] [rate_keep|normal]`

【参数说明】

参数	说明
portlist	表示端口列表，可以对多个端口同时操作
all	表示对所有端口操作
rate_keep	速率保持模式
normal	普通模式

【使用指导】缺省值为普通模式。

【配置实例】配置端口 1 的同步失败后模式为 rate_keep 模式。

```
Harbour(config)# config fail-sync-mode 1 rate_keep
```

查看局端速率的同步失败后模式

【命令语法】`show fail-sync-mode [<portlist>|all]`

【配置实例】

Harbour(config)# show fail-sync-mode 1

Port 1: fail-sync-mode is rate_keep

3.12 查看端口的 VDSL 链路的收发包信息

【命令语法】`show vdsl [<portlist>|all] [modem|switch] stats`

【参数说明】

参数	说明
portlist	表示端口列表，可以对多个端口同时操作
all	表示对所有端口操作
modem	表示 CPE 端的收发信息
switch	表示局端的收发信息

【配置实例】

Harbour(config)# show vdsl 1 modem stats

Vdsl Port: 1 Modem's Statistics Information

Rx Octets ok : 936 Tx Octets ok : 0

Rx valid frames : 4 Tx valid Frames : 0

Rx Pause frames : 0 Tx Pause frames : 0

Rx Broadcast frames : 4

Receive errors frames(<64 bytes) : 0

Reed Solomon error : 0

Alignment errors frames : 0

Single Collision Frames : 0

Multiple Collision Frames : 0

Deferred Transmission : 0

Late Collisions : 0

Excessive Collisions : 0

Carrier Sense Errors : 0

Frame Too Long Errors : 0

FCS errors : 0

3.13 端口命令列表

表 3-1：端口配置命令表

命令	描述
config port [<portlist>|all] [enable|disable]	使能或禁用指定的端口
config port [<portlist>|all] auto [on|off]	使能或禁用端口的自适应功能
config port [<portlist>|all] speed [10|100]	切换指定端口的速度至 10 Mbps 或者 100Mbps
config port [<portlist>|all] duplex [full|half]	设置端口的双工模式为全双工或者半双工
config port [<portlist>|all] flowcontrol [on|off]	使能或禁用指定端口的流控制功能
config port [<portlist>|all] learning [enable|disable]	使能或禁用指定端口的自学习功能属性
show port [<portlist>|all] {[configuration|stats]}*1	显示端口的信息 输入 configuration 选项时显示端口配置信息 输入 stat 选项时显示端口流量统计信息 缺省不输入任何选项时显示端口配置信息
config port [<portlist>|all] summary [<details|normal>]	配置端口的概要信息
config modem [<modemlist>|all] [upstream|downstream|both] rate [R16.67|R12.5|R8.33|Rom|R1.04|R4.17|R2.08|R9.38]	设置 VDSL 端口的速率等级，分别为 16.67Mbps、 12.5Mbps、 8.33Mbps、Rom、1.04Mbps、4.17Mbps 、2.08Mbps、和 9.38Mbps 的速率
config modem < modemlist > [SERIAL_NO|HARDWARE_VERSION|SOFTWARE_VERSION] <string>	配置用户 Modem 的序列号、硬件版本号、软件版本号的信息

config modem [<modemlist>|all] auto [on|off]	使能或禁用指定 VDSL 端口的自适应功能
config vdsl_port [<portlist> |all] reset	软复位用户 Modem
config modem [<modemlist> | all] speed [10|100]	配置 VDSL 端口的速率至 10 Mbps 或者 100Mbps
config modem [<modemlist>|all] duplex [full|half]	配置 VDSL 端口的双工模式为全双工或者半双工
config modem [<modemlist>|all] flowcontrol [on | off]	使能或禁用 VDSL 端口 Modem 的流控制
config vdsl_port [<portlist>|all] LT_flowcontrol [on|off]	使能或禁用 VDSL 端口局端的流控制
show vdsl_port [<portlist>|all] LT_flowcontrol	显示 VDSL 端口局端的流控制
show modem[<modemlist>|all]	显示 Modem 端口的信息
show modem [<modemlist>|all] sysinfo {[SERIAL_NO|HARDWARE_VERSION|SOFTWARE_VERSION]}*1	显示 Modem 的硬件版本号、序列号、软件版本号的信息
config modem [<modemlist>|all] patch50	配置 Modem 的 Firmware
config modem [<modemlist>|all] patch56	
show modem [<modemlist>|all] patch-version	查看 Modem 的 Firmware 版本信息
config auto-update-patch [enable|disable]	配置 Modem 的 Firmware 的自动升级信息
show auto-update-patch	查看 Modem 的 Firmware 的自动升级信息
test loopback [<portlist>|all] [line]	环路测试命令
show vdsl [<portlist>|all] [modem|switch] stats	查看端口的 VDSL 链路的收发包信息
config auto_ability_of_modem [patch50|patch56] [100|10]	根据不同的 Firmware 版本对自协商最大协商能力配置
show auto_ability_of_modem [patch50|patch56]	显示不同的 Firmware 版本的 Modem 的当前最大协商能力
config pre-sync-mode [<portlist>|all] [static|dynamic]	配置局端速率的同步前模式
show pre-sync-mode [<portlist>|all]	查看局端速率的同步前模式
config fail-sync-mode [<portlist>|all] [rate_keep|normal]	配置局端速率的同步失败后模式
show fail-sync-mode [<portlist>|all]	查看局端速率的同步失败后模式
show modem [<modemlist>|all] auto_ability	显示 Modem 当前实际的最大协商能力
clear port [<portlist>|all] stats	清除端口收发包统计信息

3.14 Hammer3100 系列交换机的多端口负载均衡组(Sharing)

Hammer3100 系列交换机能通过创建多端口负载均衡组(Sharing)来提升交换机之间的带宽。Sharing 把多个物理端口捆绑在一起当作一个逻辑端口来使用。例如在 VLAN 中所看到的

Sharing 是一个逻辑端口。Sharing 同时对客户间的数据包顺序提供保障。

如果 Sharing 中的一个端口发生堵塞或故障，那么数据包会被重新分配到该 Sharing 中别的端口进行传输。如果这个坏掉的端口重新恢复正常，那么数据包将重新分配到该 Sharing 中的所有端口来进行传输。

注意：

必须在相互连接的两台交换机上都设置 Load Sharing，且主端口对应连接。

当一台交换机的两个以上端口同时要向相邻的交换机发送数据时，创建 Sharing 非常有助于提高传输速度。

Hammer3100 系列交换机支持 Load Sharing 功能，同时与 Intel 和 Cisco 同类产品的 port group 功能兼容。

3.14.1 创建 Load Sharing

要创建一个 Load Sharing，必须创建 Sharing 的一组端口。Sharing 定义必须遵从以下规则：

- 用Load Sharing连接两个交换机时，要求Switch1中Load Sharing的端口和Switch 2中Load Sharing的主端口对应连接。
- Hammer3100系列交换机只支持一个Sharing。
- 一个Sharing组中最多包含4个端口。
- 一个Load sharing组，相当于一个端口，因此在配置时，不得更改从端口的参数

定义一个 Sharing 组，可以选取其中的一个端口作为主端口，这个主端口在逻辑上代表这个 Sharing 组。创建一个 Sharing 组，利用以下命令：

【命令语法】`create sharing <mainport> grouping <portlist> {SourceDestination}*1`

【参数说明】

参数	说明
mainport	表示主端口号
portlist	表示负载均衡组中的端口列表
SourceDestination	可选，如果选择此参数，则表示负载均衡按照源和目的 MAC 地址进行。如果不选择此参数则表示负载均衡按照源 MAC 地址进行。

【使用指导】注意：当参与 Sharing 的端口有一个是 LINK 的，则主端口必须处于 LINK 状态才可以配置。

注意：

每个负载均衡组最多只能配置 4 个端口（含主端口）。

【配置实例】创建一个 Load Sharing 组，主端口号是 1，组内端口号是 2-4，配置如下：

Harbour(config)# creat sharing 1 grouping 2-4

Harbour(config)# show sharing

Sharing port group 1 information:

Master Port: 1 Group Ports: 1 2 3 4

Load sharing according as Source Mac.

在这个例子中，端口 1 在逻辑上代表物理端口 1 、2 、3 、4。

创建了 Sharing 后，您在以后配置 VLAN 时都应该以当前状态下该 Sharing 逻辑上的主端口（如上例中的端口 1 代表整个 Sharing 组中的所有端口）为准。当在进行 VLAN 配置时，对该主端口的操作等同于对该 Sharing 组中的所有端口操作。

注意：

在配置 VDSL 的 Load Sharing 时，建议在非 VDSL 端口上配置。

3.14.2 删除一个 Sharing 组

【命令语法】delete sharing <mainport>

【参数说明】参数 mainport 的取值范围同上一条命令。

3.14.3 显示 Load Sharing 配置

【命令语法】show sharing

【使用指导】该命令会显示出当前系统中正在运行的 Sharing 组信息。包括主端口以及组中所含的端口列表。

【配置实例】在交换机上配置如下：

Harbour(config)# create sharing 2 grouping 2-4

Harbour(config)# show sharing

Sharing port group 1 information:

Master Port: 2 Group Ports: 2 3 4

Load sharing according as Source Mac.

3.15 dot1p(802.1p)配置

802.1p 协议定义了优先级的概念，对于那些实时性要求很高的数据包，主机在发送时在以太网帧的帧头中增加 3 位优先级字段以指明该数据包的优先级别，这样，当以太网交换机数据发生拥塞时，为了保证高优先级的数据包优先转发，而又不至于在高优先级的包很多，而低优先级的数据包很长时间得不到发送，我们可以通过设置高低优先级数据包的比例，来解决这样的问题。

交换机支持 IEEE 802.1p VLAN Priority，提供基于端口的优先级，具有两个优先级队列,高优先级 High 和低优先级 Low。

3.15.1 配置端口的 dot1p 优先级

【命令语法】conifg port [<portlist>|all] dot1p[high|low] {[replacement]}*1

config port [<portlist>|all] dot1p high <4-7> {[replacement]}*1

config port [<portlist>|all] dot1p low <0-3> {[replacement]}*1

【参数说明】

参数	说明
portlist	表示端口列表，可以对多个端口同时操作
all	表示对所有端口操作
high	表示把端口的优先级设置为高
low	表示把端口的优先级设置为低
replacement	选择此参数表示覆盖指定端口的优先级位
<4-7>	端口的优先级值
<0-3>	端口的优先级值

【配置实例】配置端口 1 dot1p 的优先级为高，键入命令：

Harbour(config)# config port 1 dot1p high

3.15.2 配置优先级权重

通常我们在配置端口的 dot1p 优先级之后，还要配置优先级权重，以指明端口转发高低优先级数据包的比例。

【命令语法】config dot1p weight <0-126>

【参数说明】

参数	说明
<0-126>	代表高优先级与低优先级数据包的比例，如果参数设置为 10，表示端口在转发数据包时，高低优先级数据包的比例是 10：1。当参数设为 0，则发送完所有高优先级的数据包后再发送低优先级的数据包

【命令模式】 配置模式

【相关命令】show dot1p weight（显示端口的 dot1p 优先级权重）

3.15.3 显示端口的 dot1p 值

【命令语法】show port [<portlist>|all] dot1p

【参数说明】

参数	说明
portlist	表示端口列表，可以对多个端口同时操作
all	表示对所有端口操作

【命令模式】 配置模式

【配置实例】查看端口 1 的 dot1p 值，键入命令：

Harbour(config)# show port 1 dot1p

按回车，显示如下：

```
Port priority information
------------------------------------------------------------

Port  1's priority is 0
Port  1's priority replacement is not replaced

------------------------------------------------------------
```

3.16 端口 MAC 数目限定（端口安全）

本节主要包括以下内容：

- 端口的MAC限定模块概述
- MAC限定功能的配置和查看
- 端口MAC限定的命令列表

3.16.1 端口 MAC 限定功能概述

端口MAC限定的功能主要是为了增加端口的安全性，允许交换机对通过某个端口的数据包加以限制，只允许限定范围内的MAC数目通过。通常情况下，只要端口开通，从该端口上来的MAC数目是不限定的，但有时我们出于安全性的考虑，希望该端口上来的MAC不超过某个特定的数目，这时就可以打开端口MAC限定的功能，配置端口MAC限定的数目。当用户登录时，交换机首先验证该端口MAC数目的合法性，如果MAC数目超过配置的限定数目，那么就对该端口采取相应的操作，并且这种操作是可以配置的。见3.16.4和3.16.5节的内容。

3.16.2 使能端口 MAC 限定的功能并配置限定端口的数目

【命令语法】 `config port [<portlist>|all] maclimit on <1-128>`

【参数说明】

参数	说明
portlist	表示端口列表，可以对多个端口同时操作
all	表示对所有端口操作
<1-128>	限定的数目范围

【命令模式】 配置模式

【配置实例】使能 2 端口限定的功能并把 MAC 的最大数目限定为 3 个。

Harbour(config)# config port 2 maclimit on 3

3.16.3 关闭端口 MAC 限定的功能

【命令语法】`config port [<portlist>|all] maclimit off`

【参数说明】

参数	说明
portlist	表示端口列表，可以对多个端口同时操作
all	表示对所有端口操作

【命令模式】配置模式

3.16.4 端口违例处理的配置

当一个安全端口获取的 MAC 数目超过预配置的范围后，则该端口违规，违规后端口可采取的操作有 3 种，learning、halfclose、close。如果采取的操作是 learning，则端口违规后禁止端口的学习功能，此时端口不具备学习功能，新的 MAC 不能通过此端口，经过一个 waittime 周期后端口解禁，打开端口的学习功能；如果采取的操作是 halfclose，则端口违规后禁止端口，所有的 MAC 都不能通过此端口，经过一个 waittime 周期后端口解禁，重新使能端口；如果采取的操作是 close，则必须经过管理员手工操作才能使得端口解禁。

值得注意的是：在这三种违规操作下，用户都可以通过插拔 Modem 上的网线或 RJ-11 线使得违规端口 Link Down，将端口自动解禁。而在这种情况下解禁后，端口的 MAC 限定配置并未解除，交换机仍会对通过端口的 MAC 数目进行限制，如果端口违规会再次锁定端口。

端口若违例发生，在可配时间内，给予禁止学习功能或者半关闭端口的操作

【命令语法】config port [<portlist>|all] maclimit action [learning|halfclose] wait <30-214700000>

【参数说明】

参数	说明
portlist	表示端口列表，可以对多个端口同时操作
all	表示对所有端口操作
learning	禁止学习功能，在给定时间后解锁。等待硬件老化时间后，重新开始判断违例。
halfclose	禁止端口，在给定时间后使能。等待硬件老化时间后，重新开始判断违例。
<30-214700000>	指明状态至少维持时间，单位为秒。

【命令模式】配置模式

【配置实例】配置端口 2 若有违例发生，则在 40 秒内禁止端口，40 秒后解禁。

```
Harbour(config)# config port 2 maclimit action halfclose wait 40
```

端口若违例发生，禁止端口

【命令语法】 config port [<portlist>|all] maclimit action close

【参数说明】

参数	说明
portlist	表示端口列表，可以对多个端口同时操作
all	表示对所有端口操作

【使用指导】 违例发生后，端口将一直被禁止，直到管理员人工干预。

【命令模式】 配置模式

【配置实例】端口 2 若有违例发生，则禁止端口。

```
Harbour(config)# config port 2 maclimit action close
```

3.16.5 配置端口违例后是否发 Trap

【命令语法】 config port [<portlist>|all] maclimit trap [yes|no]

【参数说明】

参数	说明
portlist	表示端口列表，可以对多个端口同时操作
all	表示对所有端口操作
yes	发 Trap
no	不发 Trap

【使用指导】缺省是不发 Trap。

【命令模式】配置模式

3.16.6 查看 MAC 限定的信息

【命令语法】show port [<portlist>|all] maclimit {[detail]}*1

【参数说明】

参数	说明
portlist	表示端口列表，可以对多个端口同时操作
all	表示对所有端口操作
detail	如果有 detail 参数，则显示详细信息

【使用指导】查看 MAC 限定的信息。

【命令模式】只读模式

【配置实例 1】

Harbour(config)# sh port 2 maclimit

port 2

mac limit :6 . learning : 6

action :halfclose . waittime : 300 . trap no

softstate :lock . hwstate : disable and lock

说明：

mac limit：表示用户配置最多学习 6 个 MAC；

learning ：表示已学习了 6 个 MAC；

action ：表示用户配置的违例动作；

waittime ：表示用户配置的违例动作至少维持时间；

softstate ：端口的软件状态，共三种：normal、learning、lock；

hwstate ：端口的硬件状态，指学习功能及 STP 的硬件状态。

学习功能状态有：lock、unlock。

STP 状态有：disable、learning、listening、forwording。

【配置实例 2】

```
Harbour(config)# sh port 2 maclimit detail
port 2
mac limit :6            . learning    : 6
action    :halfclose   . waittime    : 300   . trap no
softstate :lock         . hwstate     : disable and lock
port 2 elapsed time 58   s exceptioncouter 0
mac list:
00:01:30:55:98:e2 pos:0
00:50:fc:20:3f:85 pos:96
00:05:3b:00:26:e0 pos:140
00:10:dc:5c:79:92 pos:166
00:20:ed:a6:de:ce pos:190
00:01:e6:37:85:3d pos:192
total: 6 items
execpt mac:
total: 0 items
```

说明：

elapsed time：表示最后一次对端口状态改变迄今的时间；

exceptioncouter：表示该端口的软件 FDB 表中因 Hash 冲突无法在 hash 表中保存的 MAC 地址数目；

mac list： 端口软件 FDB 表的 Hash 表中已学习到的 MAC 地址数目；

Pos： 该条地址在 Hash 表中的位置；

execpt mac： Hash 冲突地址列表。

3.16.7 端口 MAC 限定的命令列表

命令	描述

config port [<portlist>|all] maclimit on <1-128>	使能端口 MAC 限定的功能并配置限定端口的数目
config port [<portlist>|all] maclimit off	关闭端口 MAC 限定的功能
config port [<portlist>|all] maclimit action [learning|halfclose] wait <30-214700000>	端口若违例发生，在可配时间内，给予禁止学习功能或者半关闭端口的操作
config port [<portlist>|all] maclimit action close	端口若违例发生，禁止端口
config port [<portlist>|all] maclimit trap [yes|no]	配置端口违例后是否发 Trap
show port [<portlist>|all] maclimit {[detail]}*1	查看 MAC 限定的信息

3.17 Hammer3100 系列交换机的端口镜像(Mirror)

端口镜像将通过一个或多个端口的数据复制到指定的交换机端口上，从而可进行网络流量分析和错误诊断等。

Hammer3100 系列交换机支持端口镜像功能，在 Hammer3100 系列交换机上，端口镜像功能基于如下规则：

- 每一个设备中，只能将一个端口作为镜像的目标端口。
- 可以将多个端口镜像到一个端口。

3.17.1 配置镜像目标端口

本交换机只支持一个镜像目标端口，通过以下命令配置。

【命令语法】config mirroring to <portnumber>

【参数说明】

参数	说明
portnumber	指定的镜像目标端口，可以是交换机中的任意一个端口。

【配置实例】将镜像目标端口设置为 2，键入命令：

Harbour(config)#config mirroring to 2

3.17.2 配置参与镜像的源端口

通过以下命令，增加或者删除参与镜像的源端口

【命令语法】config mirroring [add|delete] port [<portlist>|all]

【参数说明】

参数	说明
add	添加数据源端口
delete	删除数据源端口
portlist	添加或者删除指定的镜像源端口的列表。（除了镜像目标端口）
all	添加或者删除所有的镜像源端口

【配置实例】将镜像目标端口配置为 2 之后，向该镜像目标端口添加数据源端口 3-6

Harbour(config)#config mirroring add port 3-6

此时，通过端口 3-6 的数据包全部从 2 端口通过，这样可以通过截取端口 2 的数据包达到诊断错误的目的。

从该镜像端口删除数据源端口 3 时，键入命令：

Harbour(config)#config mirroring delete port 3

3.17.3 显示端口镜像配置信息

【命令语法】show mirroring

【配置实例】

Harbour(config)#config mirroring to 2

Harbour(config)#config mirroring add port 3-6

Harbour(config)# show mirroring

按回车，信息显示如下：

Mirroring information:

The port which traffic mirror to : 2.

The ports which traffic mirror from : 3 4 5 6

3.17.4 取消端口镜像功能

【命令语法】config mirroring disable

第4章 虚拟局域网 VLAN

在交换机上设置虚拟局域网络 Virtual Local Area Networks （VLAN）能使网络管理员的配置管理工作变得轻松。这一章主要讲述 VLAN 的相关概念，并说明如何在 Hammer3100 系列交换机上设置 VLAN 的各项属性。

4.1 VLAN 概述

VLAN 主要指看起来好像在同一个物理局域网中通信的设备集合。任何一个端口的集合（甚至交换机上的所有端口）都可以被看作是一个 VLAN。VLAN 的划分不受硬件设备物理连接的限制，用户可以通过命令灵活地划分端口，创建定义 VLAN。具体来说，使用 VLAN 有如下好处：

- VLAN能帮助控制流量

在传统网络中，不管是否必要，大量广播数据被直接送往所有网络设备，从而导致网络堵塞。而 VLAN 能设置每个 VLAN 中只包含那些必须相互通信的设备，从而减少广播，提高网络效率。

- VLAN提供更高的安全性

在每个 VLAN 中的设备只能与在同一 VLAN 中的设备通信。例如，如果在市场部的 VLAN Market 中的设备必须跟销售部的 VLAN Sales 中的设备通信时，就必须通过路由设备才能进行。这样，两个部门就不能直接通信，从而提高系统安全性能。

- VLAN使网络设备的变更和移动更加方便

在传统网络中，网络管理员不得不在网络设备的变更和移动上花费大量的时间和精力。如果用户移动到另一个不同的子网，那么每个终端的地址都得重新设置。而使用 VLAN 则不需要这些复杂繁琐的设置。

4.2 VLAN 的分类

本交换机最多支持 32 个 VLAN。用户可以根据以下标准创建 VLAN：

- 物理端口
- 802.1Q tag
- 以上标准的组合

4.2.1 以端口划分的 VLAN(Port-Based VLAN)

在一个 Port-Based VLAN 中，可用一个 VLAN 的名字来代表交换机中的一个或多个端口组成的一组端口。每一个端口最多只能属于一个 Port-Based VLAN 中。

4.2.2 以标签划分的 VLAN(Tagged VLAN)

标签（Tagging）就是在以太网帧中插入特定的记号（叫做 Tag）。标签通常包含某个指定 VLAN 的鉴定数字，叫做 VLANid。

注意：

使用 802.1Q 标签的数据包可能导致数据包长度比现行的 IEEE 802.3/以太网帧的最大字节数 1，518 稍微大一点。而这可能导致其他设备中的数据包计数错误，这又可能在存在非 802.1Q 的网桥或者路由器的网络中导致连接出现问题。

4.2.3 Tagged VLAN 的应用

标签（Tagging）最常应用在跨交换机创建 VLAN。交换机之间的连接通常叫做中继。使用标签后，可以通过一个或多个中继创建跨多个交换机的 VLAN。一个 VLAN 可以很轻易地通过中继跨多个交换机。

使用 Tagged VLAN 的另一个好处就是一个端口可以属于多个 VLAN。这一点在当您有一个设备（例如服务器）必须属于多个 VLAN 的时候特别有用。这个设备必须有支持 802.1Q 的网络接口卡 Network Interface Card(NIC)。

4.2.4 指定 VLAN 标签

每一个 VLAN 都可以赋予一个 802.1Q VLAN Tag（标签）。当端口被加到一个 802.1Q 标签定义好的 VLAN 中去时，您可以决定该端口是否使用该 VLAN 的标签。Hammer3100 系列交换机的缺省模式是所有端口都属于一个名叫 default 的 VLAN 中，但是不使用该 VLAN 的标签（VLANid）-- 2047。

并不是所有端口都必须使用标签。当数据流从交换机的一个端口进入，交换机实时决定是否需将该 VLAN 的标签加入到数据包中。交换机根据每个 VLAN 端口的配置情况决定加上或者去掉数据包中的标签。

注意：

如果交换机收到带 Tag 标记的数据包，而接收数据的端口又并不属于配置带该 Tag(VLANid)的 VLAN 时，那么交换机将丢弃该数据包。

4.2.5 混合使用 Tagged VLAN 和 Port-Based VLAN

您可以混合使用 Tagged VLAN 和 Port-Based VLAN。一个给定的端口可以属于多个 VLAN。

注意：

出于 VLAN 分类的目的，如果交换机收到一个含 802.1Q 标签的数据包，但是该 802.1Q 标签所含的 VLANid 的值为０，那么交换机会把该数据包当作是未标签的（untagged）。

4.2.6 VLAN 的名字

Hammer3100 系列交换机支持 32 个不同的 VLAN。每个 VLAN 的名字可以是以字母、数字、下划线开头的１至 20 个字符组成，空格符、逗号、引号等字符都是不合法的。注意：VLAN 的名称是严格区分大小写的。

VLAN 的名字都只是本地标志。也就是说，在一台交换机上设置的 VLAN 的名字只对该交换机有意义。如果 switch1 和 switch2 相连，在 switch1 上设置的 VLAN 的名称对 switch2 来讲毫无意义。

注意：

您应该在整个网络中统一规划命名您的 VLAN。

4.2.7 缺省 VLAN(Default VLAN)

每一台交换机出厂时都有一个缺省的 VLAN，该 VLAN 有以下属性：

- VLAN 的名字是 default
- 它包含所有端口
- default VLAN的所有端口都是untagged的
- default VLAN已分配了一个VLANid是2047。

4.3 配置 VLAN

这一小节主要讲述在交换机上配置 VLAN 的相关命令。

配置 VLAN 包括以下几步：

- 创建VLAN并给该VLAN取名
- 给VLAN指定一个Tag（或者使用创建时系统分配的Tag）
- 在VLAN中加入端口，当您加入端口时可以指定是否使用802.1Qtag
- 配置VLAN的inputport来改变VLAN中端口的defaultVID。

表 4-2 配置 VLAN 的相关命令

命令	描述
create vlan <name>	创建一个名为<name>的 VLAN
delete vlan {<name>}*1	删除一个名为<name>的 VLAN，或删除所有

	VLAN（除缺省 VLAN 外）
config vlan <name> tag <1-4095>	指定 VLAN 的 Tag，即 VLANid。
config vlan <name> inputport <portlist>	配置指定 VLAN 的端口,使这些端口用该 VLAN 的 VID 做为自己的 defaultVID。
config vlan <name> [add|delete] port <portlist> [tagged|untagged]	在 VLAN 中增加或删除端口,并设置该端口是 Tag 还是 untagged。
config vcn up <portlist> [notagout|tagout] baseVID <1-4069>	为交换机的所有端口（除上行端口外）分别创建一个 VLAN，端口之间隔离开来，不能相互通信，只能和用户指定的上行端口通信。
config vlan [<name>|all] console [enable | disable]	配置 VLAN 的 Console 管理功能，如果选择 disable 则该 VLAN 内的所有端口将不能再管理交换机

4.3.1 创建 VLAN

【命令语法】 create vlan <name>

【参数说明】

参数	说明
name	要创建的 VLAN 名

【使用指导】 此命令用于创建一个名为<name>的 VLAN。

【命令模式】 配置模式

【配置实例】 创建一个名为 market 的 VLAN。

```
Harbour(config)# create vlan market
```

您可以使用 show vlan {<name>}*1 命令来查看交换机当前的 VLAN 信息，不输入<name>则显示所有 VLAN 信息，输入某个 VLAN 的名称<name>则只显示该 VLAN 的信息。例如显示所有 VLAN 信息，如下：

```
Harbour(config)# show vlan

VLAN ID         : 2047
Name            : default
Mac address      : 00:05:3b:00:00:00
Flag            :
Untagged Ports   : 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19
 20 21 22 23 24
```



```
VLAN ID         : 2046
Name            : market
Mac address      : 00:05:3b:00:00:00
Flag            :
Untagged Ports  :
```

从上面的例子可以看到，VLANID 为 2047 的 VLAN 是系统默认的 VLAN，VLANID 为 2046 的 VLAN 是我们刚刚创建的 VLAN market。

4.3.2 指定 VLAN 的 Tag 值

在上一节创建 VLAN market 时，系统自动为其分配一个 VLANID 2046，您也可以利用以下命令来指定 VLAN 的 Tag 值。如果两台交换机中的某些指定端口要划分到同一个 VLAN 中，则两台交换机中的相应 VLAN 的 Tag 值必须相同。

【命令语法】 config vlan <name> tag <1-4095>

【参数说明】

参数	说明
name	VLAN 名
1-4095	Tag 值的范围

【命令模式】 配置模式

【配置实例】 将名为 market 的 VLAN 的 Tag 值指定为 3200。

Harbour(config)# config vlan market tag 3200

4.3.3 配置 VLAN 的端口

向 VLAN 添加/删除端口

一个端口可以在 IEEE 802.1Q tagged 模式下属于多个 VLAN，也可以在 untaged 模式下属于多个 VLAN，使用以下命令向 VLAN 添加/删除端口：

【命令语法】 config vlan <name> [add|delete] port <portlist>[tagged|untagged]

【参数说明】

参数	说明
name	VLAN 名
add	向 VLAN 添加端口
delete	从 VLAN 中删除端口
portlist	要添加/删除的端口

tagged	向 VLAN 中添加 tagged 端口
untagged	向 VLAN 中添加 untagged 端口

【命令模式】 配置模式

【配置实例】 将端口 1－5 以 untagged 方式添加到名为 market 的 VLAN 中。

```
Harbour(config)# config vlan market add port 1-5 untagged
```

指定端口的 defaultVID

当端口以 untagged 方式属于多个 VLAN 时，每个端口只能有唯一的一个 defaultVID。端口的 defaultVID 为该端口所属的多个 VLAN 中的其中一个 VLAN 的 VID。这样当端口收到不带 Tag 值的数据帧时，会在该端口的 defaultVID 所属的 VLAN 中转发。

每个端口的缺省 defaultVID 为 default VLAN 的 VID(2047)，可以通过配置 VLAN 的 inputport 来改变 VLAN 中端口的 defaultVID：

【命令语法】 config vlan <name> inputport <portlist>

【参数说明】

参数	说明
name	VLAN 名
portlist	该 VLAN 的某个或某几个端口的端口号

【使用指导】执行完该命令时，这些端口的 defaultVID 将变为此 VLAN 的 VID。

【命令模式】 配置模式

【配置实例】 将 VLAN market 中端口 4 的 defaultVID 改为本 VLAN 的 VID。

```
Harbour(config)# config vlan market inputport 4
```

执行完此命令后，端口 4 的 defaultVID 被改成 VLAN market 的 VID。通过 show port 4 命令可以查看端口的 defaultVID 信息：

```
Harbour(config)# show port 4
--------------------------------------------------------------
              Port:4 's Configuration Information

Link state       : Down           Port state      : Disabled
AutoNegotiation : Enabled          Speed           : 10BaseT
Duplex           : Half           FlowControl     : Disabled
Learning         : Enable         Tagout          : Disable
```

```
Port Default VID: 3200          Vlan name      : market
--------------------------------------------------------------
```

4.3.4 删除 VLAN

【命令语法】 `delete vlan {<name>}*1`

【参数说明】

参数	说明
name	要删除的 VLAN 的名称

【配置实例】删除所有的 VLAN，键入命令：

```
Harbour(config)# delete vlan
```

4.3.5 更改 VLAN 的名字

【命令语法】rename vlan from <name> to <name>

【参数说明】

参数	说明
name	第一个 name 参数表示 VLAN 原来的名称，第二个 name 参数表示更改后的 VLAN 名称

【配置实例】创建一个名称为 wang 的 VLAN，并将端口 1－12 以 untagged 方式加入该 VLAN，然后改变 VLAN 的名称为 yang，配置如下：

```
Harbour(config)#create vlan wang
Harbour(config)#config vlan wang add port 1-12 untagged
Harbour(config)# rename vlan from wang to yang
```

4.3.6 配置 VLAN 的 Console 管理功能

Hammer3100 系列交换机提供了 Console 口的管理功能配置命令，当一个 VLAN 的 Console 功能被配置为 disable 后，则通过此 VLAN 的所有端口将不能 ping 通交换机的 IP 地址，从而不能通过 Telnet、Web 等手段管理交换机。增加了交换机的安全性。

【命令语法】config vlan [<name>|all] console [enable|disable]

【参数说明】

参数	说明
name	VLAN 的名称

all	表示对所有的 VLAN 进行操作
enable	使 VLAN 处于正常状态，不进行 VLAN 的 Console 口配置功能管理
disable	进行 VLAN 的 Console 口管理功能

【使用指导】选择 disable 进行 VLAN 的 Console 口管理功能时，通过 show vlan 命令可以看到 VLAN 的 Fag 的 Console 标志已经去掉了，通过该 VLAN 不能再 ping 通交换机的 IP，也就是禁止了通过 Telnet、Web 等手段管理交换机。从而增加了交换机的安全性。

【命令模式】 配置模式

【配置实例】配置交换机的 IP 为 11.11.11.1/24，PC 与交换机的 24 口相连。IP 地址为 11.11.11.11/24。配置如下：

```
Harbour(config)#config ip 11.11.11.1/24
Harbour(config)#creat vlan wang
Harbour(config)#config vlan wang add port 24 untagged
Harbour(config)#show vlan

VLAN ID        : 2047
Name           : default
Mac address     : 00:05:3b:20:01:3c
Flag           : Console
Tagged Ports    :
Untagged Ports : 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19
 20 21 22 23 24

VLAN ID        : 2046
Name           : wang
Mac address     : 00:05:3b:20:01:3c
Flag           : Console
Tagged Ports    :
Untagged Ports : 24

Harbour(config)#ping 11.11.11.11

PING 11.11.11.11 : 56 data bytes.
Press Ctrl-c to Stop.
```

```
Reply from 11.11.11.11 : bytes=56: icmp_seq=0 ttl=128 time=0 ms
Reply from 11.11.11.11 : bytes=56: icmp_seq=1 ttl=128 time=0 ms
Reply from 11.11.11.11 : bytes=56: icmp_seq=2 ttl=128 time=0 ms
Reply from 11.11.11.11 : bytes=56: icmp_seq=3 ttl=128 time=0 ms

----11.11.11.11 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss

round-trip(ms) min/avg/max = 0/0/0
```

此时可以 ping 通 PC。也就是可以通过该 VLAN 中的端口管理交换机。

```
Harbour(config)#config vlan wang console disable
Harbour(config)#ping 11.11.11.11

PING 11.11.11.11 : 56 data bytes.
Press Ctrl-c to Stop.

Reply from 11.11.11.11 : bytes=56: icmp_seq=0 ttl=128 time=0 ms
Reply from 11.11.11.11 : bytes=56: icmp_seq=1 ttl=128 time=0 ms
Reply from 11.11.11.11 : bytes=56: icmp_seq=2 ttl=128 time=0 ms


----11.11.11.11 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss

round-trip(ms) min/avg/max = 0/0/0
```

此时仍然可以 ping 通 PC。虽然此时 Console 的管理功能已经 disable 了，但是端口 24 没有指定 defaultVID，所以端口默认的 VLAN 还是 default，不管是否隔离了 VLAN wang，还是可以 ping 通 PC。

```
Harbour(config)#config vlan wang input 24
Harbour(config)#show vlan wang

VLAN ID        : 2046
Name           : wang
```



```
Mac address    : 00:05:3b:20:01:3c
Flag          :
Tagged Ports   :
Untagged Ports : 24
```

注意此时 Flag 标识中已经去掉了 Console 标识，表明 VLAN wang 已经通过 Console 禁用了管理交换机的功能。

```
Harbour(config)#ping 11.11.11.11

PING 11.11.11.11 : 56 data bytes.
Press Ctrl-c to Stop.

Request time out.
Request time out.

----11.11.11.11 PING Statistics----
2 packets transmitted, 0 packets received, 100% packet loss
```

此时已经 ping 不通 PC。

4.3.7 端口隔离批处理命令

端口隔离批处理命令将交换机的所有端口(用户指定的上行端口除外)进行隔离，使端口彼此间不能相互通信，只能和上行端口通信。

【命令语法】 config vcn up <portlist> [notagout|tagout] baseVID <1-4069>

【参数说明】

参数	说明
portlist	表示指定哪个端口作为上行通信端口，可以指定一个或两个上行端口
notagout	表示上连端口以 untag 方式属于 vcn 所创建的所有 VLAN
tagout	表示上连端口以 tag 方式属于 vcn 所创建的所有 VLAN
1-4069	表示 baseVID 的值，其中 baseVID 为最小端口号所属 VLAN 的 Tag 值，其余端口所属 VLAN 的 Tag 值为该 baseVID 加上该端口与最小端口的差

【命令模式】 配置模式

【配置实例】配置端口隔离，设定 baseVID 为 200，键入命令：

```
Harbour(config)#config vcn up 1-5 tagout baseVID 200
Harbour(config)#show vlan

VLAN ID        : 2047
Name           : default
Mac address    : 00:05:3b:20:01:3c
Flag           : Console
Tagged Ports   :
Untagged Ports : 1  2  3  4  5  6  7  8  9  10 11 12 13
14 15 16 17 18 19 20 21 22 23 24

VLAN ID        : 205
Name           : VcndVlan6
Mac address    : 00:05:3b:20:01:3c
Flag           :
Tagged Ports   : 1  2  3  4  5
Untagged Ports : 6

VLAN ID        : 206
Name           : VcndVlan7
Mac address    : 00:05:3b:20:01:3c
Flag           :
Tagged Ports   : 1  2  3  4  5
Untagged Ports : 7
```

………………………………………………（这里略去部分显示内容）

```
VLAN ID        : 223
Name           : VcndVlan24
Mac address    : 00:05:3b:20:01:3c
Flag           :
Tagged Ports   : 1  2  3  4  5
Untagged Ports : 24

VLAN ID        : 200
Name           : VcnuVlan1
```

```
Mac address    : 00:05:3b:20:01:3c
Flag           : Console
Tagged Ports    : 1  2  3  4  5
Untagged Ports : 6  7  8  9  10 11 12 13 14 15
16 17 18 19 20 21 22 23 24
```

4.4 VLAN 两种模式的配置和查看

在 Hammer3100 系列交换机上，有两种定义的 VLAN 模式可配：

A.normal：为普通模式，端口可以以 untag 方式属于多个 VLAN

B.extension：为扩展模式，端口以 untag 方式只能属于一个 VLAN。

4.4.1 VLAN 两种模式的配置

【命令语法】 config vlan mode [normal|extension]

【参数说明】

参数	说明
[normal|extension]	配置的 VLAN 模式，默认模式为 normal

【命令模式】 配置模式

4.4.2 查看 VLAN 模式

【命令语法】 show vlan mode

【使用指导】 因为命令行的匹配问题，该命令必须用“ show vlan mode ”

【命令模式】 只读模式

【配置实例】

Harbour(config)# show vlan mode

vlan mode is extension

注意：

在扩展（extension ）VLAN 模式下，对 vcn 创建的 VLAN 的操作将不被保存。因为任何对该 VLAN 的操作都是违背 vcn 命令本意的。

第5章 FDB 表

5.1 FDB 地址表概述

网络设备都以 MAC 地址来唯一地标识自己，而交换机要实现设备之间的通信必须知道自己的哪个端口上连接着哪台设备，因此特别需要一张 MAC 地址与端口号一一对应的表，以便在交换机内部实现二层数据转发，这张二层转发表就是 FDB（Forwarding Database）表。

5.1.1 FDB 地址表内容

HammerOS 的 FDB 地址表数目由产品决定，本交换机可以存储最多 4K 条地址表项。每个地址表项都包含以下内容：

- 所收到的数据源设备的MAC地址
- 与所收到的数据源设备相连的端口标志
- Flag：标志

如果收到的数据帧的目的 MAC 地址不在 MAC 地址表中，那么该数据将被发送给数据源设备所属 VLAN 的所有端口。

5.1.2 FDB 地址表的地址表项类型

FDB 地址表共有三种地址表项：

动态地址表项 —— 最开始的时候，交换机中的所有 FDB 地址表中的地址表项都是动态的。如果一段时间（老化时间 Agingtime）之后设备没有数据传输，那么该地址表项就会被删除。这样能防止地址表项变得过于庞大，当确信某个设备从网络中去除后，就把该设备的地址表项删除掉。当交换机关机重启动后，所有的动态地址表项都将被删除。关于动态地址表项的生存时间的设置，请参考本章稍后有关 FDB 地址表项配置的内容。

固定地址表项 —— 如果老化时间（Agingtime）被设为０，那么该地址表项将存储在 FDB 地址表中而不会被动态删除，直到交换机关机或者重启。

永久地址表项 —— 永久地址表项将一直保存在 FDB 地址表中，即使交换机关机或者重启。永久地址表项必须由系统管理员手工设定。一个永久地址表项可以是一个单播地址，也可以是一个多播地址。所有由命令行输入的静态地址表项都将被存储为永久地址表项。Hammer3100 系列交换机最多能支持 1000 个静态地址表项。

永久地址表项一经建立，不会更改。例如，以下任何事件的发生都不会引起永久地址表项跟着变化：

- 一个VLAN被删除
- 一个VLAN的VLANid被修改
- 一个端口的模式被改变（tagged/untagged）

- 一个端口被从VLAN中删除
- 一个端口被禁用（disable）
- 一个端口被堵塞（Block）
- 一个端口down掉（link down）

5.1.3 FDB 地址表项的加入

FDB 地址表中的地址表项可以通过以下两个途径被加入：

- 交换机自学习。交换机可以根据收到的数据包的源MAC地址，收数据包的端口，收到数据包的端口所在的VLAN来自动更新FDB地址表。
- 您可以通过命令行接口手工增加地址表项到FDB地址表中。

5.2 配置 FDB 地址表

配置 FDB 地址表可以用以下命令：

命令	描述
config fdb agingtime <0-120>	设置 FDB 地址表中的地址表项老化时间，单位是秒，缺省值为 80 秒，0 代表不老化。
create fdbentry <macaddr> <portlist> {<vlanname>}*1	创建一个静态的永久地址表项。<macaddr>标志设备的 MAC 地址，如果这一个 MAC 地址相关有多个端口，那么数据包将被转发到所有目的端口。如果选择 vlanname 则在指定的 VLAN 里面创建
delete fdbentry [<macaddr> |all] {<vlanname>}*1	删除指定 MAC 地址的地址表项。
discard fdbentry <macaddr>	丢弃来自某一个 MAC 地址的信息
show fdb agingtime	显示 FDB 表项的老化时间。
show fdb all	显示所有 FDB 地址表项信息（包括静态和动态）
show fdb permanent {[mac] <macaddr>}*1	显示 FDB 永久地址表项的信息。如果不输入后面的可选项，则显示所有的静态 FDB 表信息。
show fdb dynamic {[port]<portlist>}*1 {[mac]<macaddr>}*1	显示 FDB 动态地址表项的信息。如果不输入后面的可选项，则显示所有的动态 FDB 表信息。

5.2.1 创建一个静态永久地址表项

【命令语法】`create fdbentry <macaddr> <portlist> {<vlanname>}*1`

【参数说明】

参数	说明

macaddr	标志设备的 MAC 地址，如果一个 MAC 地址相关有多个端口，那么数据包将被转发到所有目的端口
portlist	端口列表
vlanname	如果建立的 FDB 为多播表项,此处为 VLAN 的名字

【配置实例】添加一条静态地址表项到 FDB 地址表中：

```
Harbour(config)#create fdbentry 001122334455 2
```

这个静态永久地址表项具有以下属性：

- MAC 地址是 001122334455
- 端口号是 2

5.2.2 删除 FDB 表中的地址表项

【命令语法】`delete fdbentry [<macaddr> |all] {<vlanname>}*1`

【参数说明】

参数	说明
macaddr	要删除的设备的 MAC 地址
all	删除所有的 FDB 表项
vlanname	如果删除的 FDB 表项为多播表项，此处为 VLAN 的名字

【配置实例】删除静态地址表项：00E02B123456

```
Harbour(config)#delete fdbentry 00E02B123456
```

5.2.3 丢弃来自某一 MAC 地址的数据包

作为一种安全机制或应用于某种特殊环境之下．交换机将收到的来自某源 MAC 地址的数据包丢弃．而不会从任何端口将其转发出去。

【命令语法】 `discard fdbentry <macaddr>`

【参数说明】

参数	说明
macaddr	要被标记的设备的 MAC 地址

【使用指导】 使用该命令后，指定为<macaddr>的 MAC 地址将被标记非法（Illegal），于是来自该 MAC 地址的数据包将被交换机丢弃。

【命令模式】 配置模式

【配置实例】 丢弃来自 MAC 地址为 001122334455 的数据包。

```
Harbour(config)# discard fdbentry 001122334455
```

5.2.4 显示 FDB 地址表中的静态地址表项

【命令语法】show fdb permanent {[mac] <macaddr>}*1

【使用指导】当不输入 MAC 地址时，将显示本交换机 FDB 地址表中的所有的静态地址表项的信息；当输入 MAC 地址时，将显示该 MAC 地址的静态地址表项。

【配置实例】在交换机上配置如下：

```
Harbour(config)# show fdb permanent mac 001122334455


--- Begin of Permanent Address Table Information --
Mac address       Port        Flags
--------------------------------------------------
00:11:22:33:44:55   2    Permanent NotMove
---------------------------------------------------
Total 1 static mac showed.
---------End of Permanent Mac Information ---------
```

5.2.5 显示 FDB 地址表中的动态地址表项

如果想查看 FDB 地址表中的动态地址表项，可以利用以下命令：

【命令语法】show fdb dynamic {[port]<portlist>}*1 {[mac]<macaddr>}*1

【参数说明】

参数	说明
[port]<portlist>	可选项，如果选择则显示指定的端口或者端口列表的动态地址表项
[mac]<macaddr>	可选项，如果选择，表示显示指定的 MAC 地址的动态地址表项信息

【运行模式】配置模式

5.2.6 显示 FDB 中所有地址表项

显示 FDB 中所有地址表项，利用以下命令：

【命令语法】show fdb all

【配置实例】

Harbour(config)# show fdb all

```
------- Begin of Unicast Address Table Information -------

Mac address            Port   type    tocpu  move   mirror
00:05:3b:50:06:69       0     static  2      no     no
00:05:3b:ff:ef:f0       0     static  3      no     no


------- Begin of multicast Address Table Information -------

Mac address            vlan          port

------------------------------------------------------------



Total   2 unicast  mac showed.

Total   0 multcast mac showed.

---------- End of Address Table Information ----------
```

Flag标示的含义：

Port：端口号；

type：动态还是静态地址表项；

tocpu：判断是否送到CPU处理及CPU接受该MAC上来包的优先级，从0到3优先级依次上升；

move：FDB表存放的位置是否可移动；

mirror：没有用到这个功能。

5.2.7 显示 FDB 地址表的统计信息

【命令语法】show fdb summary

【配置实例】

Harbour(config)# show fdb summary

```
Total unicast FDB entry        : 5
      static FDB entry         : 2
      dynamic FDB entry        : 3
```

Total multicast FDB entry : 0

5.2.8 配置 FDB 地址表老化时间

【命令语法】config fdb agingtime <0-120>

【参数说明】

参数	说明
0-120	单位是秒，缺省值为 80 秒,0 代表不老化

第6章 STP 协议

本章包括如下内容：

- STP协议介绍
- STP的相关配置
- 显示STP状态

6.1 STP 概述

交换机支持 IEEE802.1D 标准的 STP（Spanning Tree Protocol）协议，提供了网络的动态冗余切换机制。STP(生成树协议)使您能在网络设计中部署备份线路，当有物理环路发生时，交换机可以通过生成树协议算法，构造一个唯一的树结构，使某些端口处于 Block 状态，从而避免了环路的发生。通过这种机制，它确保到每个目的地只有一条路径，如果某条链路失效了，根网桥知道存在冗余链路，他会启动先前关掉的这条冗余链路。

STP 协议是通过在一个扩展的局域网中参与 STP 的所有交换机之间交换 BPDU 数据来实现的。BPDU（Bridge Protocol Data Units）即桥协议数据单元。通过交换 BPDU 消息可以实现：

- 为稳定的生成树拓扑结构选择一条根桥。
- 为每个交换网段选择一台指定交换机。
- 通过将冗余的交换机端口置为Blocking来消除网络中的环路。

生成树协议可以保证：

- 在主线路正常工作时，备份线路是禁用的。
- 当主线路出现故障时自动使能备份线路，切换数据流。

注意：

STP 协议在 IEEE802.1D 标准中有详细的描述。

6.2 配置 STP

在交换机上配置 STP 包含以下内容：

- 使能或禁用STP
- 使能或禁用STP的端口
- 配置指定的STP的参数

6.2.1 使能或禁用 STP

【命令语法】config stpd default [enable|disable]

【参数说明】

参数	说明
enable	使 STP 有效
disable	使 STP 无效

【使用指导】STP 缺省状态是禁用的。

6.2.2 使能或禁用指定 STP 的端口

【命令语法】config stpd default port [<portlist>|all] [enable|disable]

【参数说明】

参数	说明
portlist	所要操作的端口列表
all	表示对所有端口进行操作
enable	使该端口的 STP 有效
disable	使该端口的 STP 无效

【使用指导】所有端口默认都是参与 STP 计算的。

【命令模式】配置模式

【配置实例】使能端口 6 的 STP 功能，在配置模式下，键入命令：

Harbour(config)#config stpd default port 6 enable

按回车，执行该命令。

6.2.3 使能或禁用指定 STP 的端口逆转功能

【命令语法】config stpd default reverse [enable|disable]

【参数说明】

参数	说明
enable	表示使该端口的 STP 逆转功能有效
disable	使该端口的 STP 逆转无效

【使用指导】默认端口逆转是禁用的

【命令模式】配置模式

6.2.4 配置指定 STP 的参数

一旦运行某个指定 STP 的协议后，您可能需要根据具体的网络结构调整该 STP 的一些参数。以下的 STP 协议参数可以在 Hammer 交换机中调整：

- Bridge Priority
- Hello Time
- Forward Delay
- Max Age

另外每个端口上有以下参数可以调整：

- Path Cost
- Port Priority

下表列出了 STP 的所有配置命令。

表 6-1 STP 配置命令列表

命令	解释
config stpd default [enable|disable]	使能或禁用 STP
config stpd default priority <0-65535>	设置运行 STP 协议时本交换机的优先级。优先级的取值范围是 0-65535，缺省值为 32768。 优先级数值越低，越有可能成为网络中的根桥（Root Bridge）。优先级值为 0 代表了最高的优先级。
config stpd default hellotime <1-10>	设置当本交换机被选为根桥时发送 BPDU 的时间间隔。 HelloTime 的取值范围是 1-10，单位为秒，缺省值是 2 秒。 注意：HelloTime 必须小于等于 ForwardDelay－2
config stpd default forwarddelay <4-30>	设置当本交换机被选为根桥时端口状态切换的时间间隔。 ForwardDelay 的取值范围是 4-30，单位秒，缺省值为 15 秒。 注意：ForwardDelay 的时间必须大于等于 HelloTime+2
config stpd default maxage <6-40>	设置 BPDU 报文老化的最长时间间隔，收到超过这个时间的 BPDU 报文，就直接丢弃。 MaxAge 的取值范围是 6-40，单位为秒，缺

	省值为 20 秒。 注意：Maxage 的时间必须大于等于 2*(HelloTime + 1)，小于等于 2*(ForwardDelay – 1)
config stpd default port [<portlist>|all] [enable|disable]	指定参与 STP 协议计算的端口。
config stpd default port [<portlist>|all] priority <0-255>	配置参与 STP 计算的端口的优先级。 端口优先级的取值范围是 0-255，缺省值是 128。 优先级数值越低，端口越容易成为根端口（Root Port），优先级值为 0 代表了最高的优先级。
config stpd default port [<portlist>|all] cost <1-65535>	配置参与 STP 计算端口的路径开销。 取值范围是 1-65535，HammerOS 根据端口的当前速度设置不同的缺省值： 10Mbps 端口缺省值为 100 100Mbps 端口缺省值为 19 1000Mbps 端口缺省值为 4
config stpd default reverse [enable|disable]	该命令配置 stpd default 的端口号反向，使原来的最小的端口号变为最大的端口号，这样就改变了每个端口的 id 值，因为上行端口的端口号比较大，在其他条件相同的情况下，为了保证在进行 STP 计算后上行端口不会因此而变成 Blocking 状态，通过此命令可以使上行端口的 portID 变小。选择参数 enable 表示使能 stpd default 反向功能，选择 disable 表示禁用 stpd default 反向功能。

6.2.5 显示 STP 状态

STP 的显示内容包括：

- BridgeID
- Root BridgeID
- STP的各种配置参数

端口的 STP 显示内容包括：

- 端口状态
- Designated port
- 端口的各种配置参数

【命令语法】show stpd default {port [<portlist>|all]}*1

【配置实例 1】显示 STP 状态

```
Harbour(config)# show stpd default
STP Domain default information
------------------------------------------------------------
-- Designated Root Info --
Priority             : 32768
Mac address           : 00:05:3b:00:00:00
Max Age              : 20
Hello Time            : 2
Forward Delay          : 15

-- Bridge Info --
Priority             : 32768
Mac address           : 00:05:3b:00:00:00
Root Path Cost         : 0
Root Port            : 0
Bridge Max Age         : 20
Bridge Hello Time       : 2
Bridge Forward Delay : 15
------------------------------------------------------------
```

【配置实例 2】显示端口的 STP 状态

```
Harbour(config)# show stpd default port 2

---------------------------------------------------
Port:2 's Spanning Tree Protocol Information
-- Port Info --
Port id                 : 2
Priority                : 128
State                   : Disable
Path Cost               : 100
Designated Cost         : 0

-- Designated Port --
Port id                 : 2
```

```
Priority            : 128

-- Designated Root --
Priority            : 32768
Mac address         : 00:05:3b:00:00:00

-- Designated Bridge --
Priority            : 32768
Mac address         : 00:05:3b:00:00:00

---------------------------------------------------
```

第7章 IGMP Snooping 配置

本章包括如下内容：

- IGMP Snooping介绍
- IGMP Snooping的相关配置
- 显示 IGMP Snooping 的配置信息

7.1 IGMP Snooping 概述

本交换机支持 IGMP Snooping 功能。IGMP Snooping, 顾名思义就是一种能使交换机 " 监听 " 主机和路由器之间的 IGMP 协议通信的功能。 当交换机截取到属于某一多播组的主机 IGMP 报文时，交换机将把该主机所接端口加入到其多播组表项中，并在 FDB 表中添加此多播地址。当截取到 IGMP 离开报文时，交换机将该主机所接端口从其多播组表项中删除。

在缺省情况下，由于多播地址不可能出现在报文的源地址中，所以交换机无法学习到多播地址，因此在一个 VLAN 中，多播包将以广播的方式发送到所有端口。通过使用 IGMP Snooping 功能，可以有效地控制多播通信在广播域中的报文广播问题，使多播包只发送给在多播组中的端口，而不是所有的端口。从而，节省了大量的带宽，提高了交换机的交换效率。

7.1.1 使能或者禁用 IGMP Snooping 功能

【命令语法】igmp-snooping disable

igmp-snooping enable

【参数说明】

参数	说明
enable	使能 IGMP Snooping 功能
disable	禁用 IGMP Snooping 功能

7.1.2 配置 IGMP Snooping 超时间隔

IGMP Snooping 包含两种超时间隔：路由器超时间隔和主机超时间隔。

路由器的超时间隔，配置命令如下：

【命令语法】 igmp-snooping router_timeout <10-2147483647>

【参数说明】

参数	说明
10-2147483647	超时间隔的范围，单位是秒，缺省值是 260 秒

【命令模式】 配置模式

主机的超时间隔，配置命令如下：

【命令语法】 `igmp-snooping host_timeout <10-2147483647>`

【参数说明】

参数	说明
10-2147483647	超时间隔的范围，单位是秒，缺省值是 260 秒

【命令模式】 配置模式

7.1.3 清除 IGMP Snooping 信息

清除某个 VLAN 中或所有 VLAN 中的组成员，可在配置模式下使用以下命令：

【命令语法】 `clear igmp snooping vlan <name>`

或者

`clear igmp snooping vlan all`

【参数说明】

参数	说明
name	指定 VLAN 的名称
all	代表所有的 VLAN

【命令模式】 配置模式

【配置实例】 清除 default 中的所有组成员关系。

```
Harbour(config)# clear igmp snooping vlan default
```

7.1.4 指定可以创建组播组的 VLAN

默认状态下，组播组的创建是在 default VLAN 中创建的，我们也可以通过命令改变可以创建组播组的 VLAN，配置如下命令后，组播组只能在我们指定的 VLAN 中创建，不能在其他 VLAN 中创建。

【命令语法】config vlan <name> igmpport <portlist>

【参数说明】

参数	说明
name	指定 VLAN 的名称

portlist	端口的列表

【命令模式】 配置模式

7.1.5 显示 IGMP Snooping 信息

显示指定 VLAN 中或所有 VLAN 中的组播组成员信息，可使用以下命令：

【命令语法】 show igmp snooping vlan [<name>|all]

【参数说明】

参数	说明
name	指定 VLAN 的名称
all	表示所有的 VLAN

【命令模式】 配置模式

【配置实例】

```
Harbour(config)# show igmp snooping vlan all
VLAN ID         : 2047
Name            : default
Mac address     : 01:00:5e:03:04:01
Ports           : 5  10

VLAN ID         : 2047
Name            : default
Mac address     : 01:00:5e:03:04:02
Ports           : 5

VLAN ID         : 2047
Name            : default
Mac address     : 01:00:5e:7f:ff:fe
Ports           : 5  22
```

7.1.6 显示端口所在 IGMP Snooping 的 VLAN ID

【命令语法】show igmp port [<portlist>|all]

【参数说明】

参数	说明
portlist	表示端口列表，可以选择多个端口
all	表示选择所有的端口

【命令模式】配置模式

【配置实例】

Harbour(config)# show igmp port 21

```
Port 21 's igmp vlan ID : 2047
```

7.1.7 使能或者禁用 IGMP Snooping 立即离开功能

【命令语法】igmp-snooping immediate-leave [enable|disable]

【参数说明】

参数	说明
enable	表示使能 igmp-snooping 立即离开功能
disable	表示关闭 igmp-snooping 立即离开功能

【使用指导】当组中的一个成员离开时立即将消息发送给 IGMP-Snooping 路由器，使其立即离开，该功能适用于对快速离开要求严格的地方。

7.2 IGMP Snooping 命令表

表 7-1 IGMP Snooping 的配置命令

命令	描述
igmp-snooping enable	使能 IGMP Snooping 功能
igmp-snooping disable	禁用 IGMP Snooping 功能
igmp-snooping router_timeout <10-2147483647>	指定路由器超时的时间间隔（默认值为 260 秒）
igmp-snooping host_timeout <10-2147483647>	指定主机超时的时间间隔（默认值为 260 秒）
clear igmp snooping vlan [name|all]	清除某个 VLAN 中或所有的 VLAN 中的组成员信息列表
config vlan <name> igmpport <portlist>	指定可以创建组播组的 VLAN

show igmp snooping config	显示 IGMP Snooping 的配置参数
show igmp snooping vlan [name|all]	显示某个 VLAN 中或所有 VLAN 中的多播组成员
show igmp port [<portlist>|all]	显示 IGMP Snooping 端口所在的 VLAN ID

第8章 SNTP 协议

本章包括如下内容：

- SNTP协议介绍
- SNTP的相关配置
- 显示SNTP配置信息
- 使用举例

8.1 SNTP（Simple Network Time Protocol）概述

8.1.1 SNTP 协议介绍

SNTP 的全名为简单网络时间协议，它是设计来使网络中的设备能维持相同的时间的一种通信协议，通过在网络设备中运行 SNTP 协议，有利于网络中设备的管理和维护。SNTP 协议采用客户端、服务器的方式。

8.1.2 SNTP 的三种工作模式

在 Hammer3100 系列交换机上，SNTP 协议在维护网络设备的时间时工作于 Unicast 模式：

客户端通过向指定的服务器发出包含本地时间请求的报文，服务器在响应报文中包含服务器接收到客户端请求报文的时间和服务器发出响应报文的时间。客户端在收到服务器的响应报文后，通过报文中包含的各种时间值可以计算出报文的循环周期以及本地设备的时间值和服务器的偏差。

8.2 配置 SNTP

在交换机上配置 SNTP 包含以下内容：

- 配置SNTP客户端或SNTP服务器的工作模式
- 使能（使SNTP客户端有效）或关闭SNTP的客户端
- 使能（使SNTP服务器有效）或关闭SNTP的服务器
- 配置SNTP客户端的各种参数

8.2.1 使能或关闭 SNTP 客户端

【命令语法】config sntp-client [enable|disable]

【参数说明】

参数	说明
enable	表示使能运行 SNTP 客户端
disable	表示禁用运行 SNTP 的客户端

【使用指导】在一台 Hammer3100 交换机中 SNTP 客户端的缺省状态是关闭的；在启动 SNTP 客户端以前必须先配置 SNTP 的工作模式。

【命令模式】配置模式

8.2.2 配置客户端的 SNTP 服务器的 IP 地址

当 SNTP 客户端工作在 Unicast 模式下时，在启动 SNTP 之前一定要先配置 SNTP 服务器的 IP 地址，以便客户端能和指定的服务器之间进行通信。利用如下命令：

【命令语法】config sntp-client server ipaddr <A.B.C.D >

【参数说明】

参数	说明
A.B.C.D	SNTP 服务器的 IP 地址

【命令模式】配置模式

【配置实例】配置客户端的服务器的 IP 地址为 10.5.4.66

Harbour(config)# config sntp-client server ipaddr 10.5.4.66

8.3 显示 SNTP 的状态信息

【命令语法】show sntp-client {[default]}*1

【使用指导】show 命令所显示的 SNTP 客户端的信息包括以下内容：

时间服务器的 IP 地址；

SNTP 是否启动；

SNTP 的默认 IP 地址（如果有参数 “ default ”）。

【配置实例】显示 SNTP 客户端的配置信息：

Harbour(config)# show sntp-client

!------------sntp client's current state--------------

sntp-client are running.

user give : 10.5.4.66

```
sntp server is in using : 10.5.4.66
Harbour(config)# show sntp-client default
!------------sntp client's current state--------------
sntp-client are running.
user give : 10.5.4.66
sntp server is in using : 10.5.4.66
default:
137.92.140.80
128.250.36.2
138.194.21.154
130.155.98.1
130.95.156.206
200.19.119.69
142.3.100.2
128.233.3.100
128.233.3.101
193.5.216.14
129.132.2.21
146.83.8.200
200.68.60.246
195.113.144.201
131.188.3.220
131.188.3.221
131.188.3.222
131.188.3.223
130.149.17.21
130.149.17.8
192.53.103.103
192.53.103.104
129.69.1.153
```

8.4 配置系统的 Timezone 信息

8.4.1 清除配置的 Timezone 信息

【命令语法】clear timezone

【命令模式】配置模式

8.4.2 配置本地时区信息

【命令语法】config timezone <name> [east|west] <0-12> {<1-59>}*1

【参数说明】

参数	说明
name	时区名称，如中国所在时区简称为：CST
east|west	指明是东半球还是西半球
0-12	指明时区号
1-59	指明本地标准时间在本时区的分钟数，一般的国家都以整时区作为标准

【命令模式】配置模式

【配置实例】

配置中国时区：

Harbour(config)# config timez CST east 8 (中国标准时间在东 8 区)

配置美国时区：

Harbour(config)# config timez USA west 5 (美国标准时间在西 5 区)

8.5 SNTP 命令列表

下表列出了 SNTP 的所有配置命令。

命令	描述
config sntp-client [enabler|disable]	使能或关闭 SNTP 协议的客户端软件
config sntp-client server ipaddr <A.B.C.D>	配置 SNTP 协议客户端的时间服务器的 IP 地址。
show sntp-client {[default]}*1	显示 SNTP 客户端的状态。
show timezone	显示系统 Timezone 信息

clear timezone	清除系统 Timezone 配置信息
config timezone <name> [east|west] <0-12> {<1-59>}*1	配置系统 Timezone 信息

第9章 NAS 接入服务

9.1 NAS 接入服务概述

随着宽带以太网建设规模的迅速扩大，为了适应用户数量急剧增加和宽带业务多样性的要求，港湾网络有限公司通过在 Hammer 系列交换机上嵌入接入服务完成用户的认证和管理功能，以便更好地支持宽带网络的计费、安全、运营和管理的要求。嵌入了接入服务的 Hammer 交换机称为网络访问服务器（Network Access Server，NAS）。

接入服务在运用 802.1x 协议和 RADIUS 协议的基础上，实现对用户接入的认证和管理功能。使用接入服务主要有以下优点：

- **简洁高效**：纯以太网技术内核，保持IP网络无连接特性，去除冗余昂贵的多业务网关设备，消除网络认证计费瓶颈和单点故障，易于支持多业务；
- **容易实现**：可在普通L3、L2、IP DSLAM上实现，网络综合造价成本低；
- **安全可靠**：在二层网络上实现用户认证，并可以通过设备实现MAC、端口、账户和密码等绑定技术，具有很高的安全性；
- **易于运营**：控制流和业务流完全分离，易于实现多业务运营。

接入服务在运用 802.1x 基于端口的访问控制协议的基础上扩展了该协议，实现了基于用户 MAC 地址的访问控制，可以对设备一个端口上的多个接入用户分别进行认证和管理，提供对用户接入的灵活控制，同时能够与动态主机配置协议中继代理（DHCP Relay）相结合，为计费服务器提供用户的 IP 地址。

接入服务提供 3 种身份验证方式：PAP，CHAP 和 EAP-MD5 方式，根据业务运营的不同需求，可以使用其中任何一种身份验证方式实现接入服务：

1．使用 PAP 方式进行身份验证

如图 9-1 所示，首先用户终端向 Hammer 交换机发送 EAPOL-START 报文请求接入服务，交换机返回 EAP-REQUEST/IDENTITY 报文到用户终端，要求用户提供身份标识，用户终端返回 EAP-RESPONSE/IDENTITY 响应报文表示连接建立。然后交换机发送 EAP-REQUEST/PAP 报文通知用户使用 PAP 方式验证身份，用户终端发送 EAP-RESPONSE/PAP 报文到交换机，该报文中含有用户名和用户密码。交换机根据来自用户终端的 EAP-RESPONSE/PAP 报文组装并发送 ACCESS REQUEST 报文到 RADIUS 服务器。RADIUS 服务器对用户进行认证，如果认证通过，返回 ACCESS ACCEPT 报文给交换机，由交换机完成相应操作以允许用户接入，同时发送 EAP-SUCCESS 报文到用户终端通知用户接入成功。

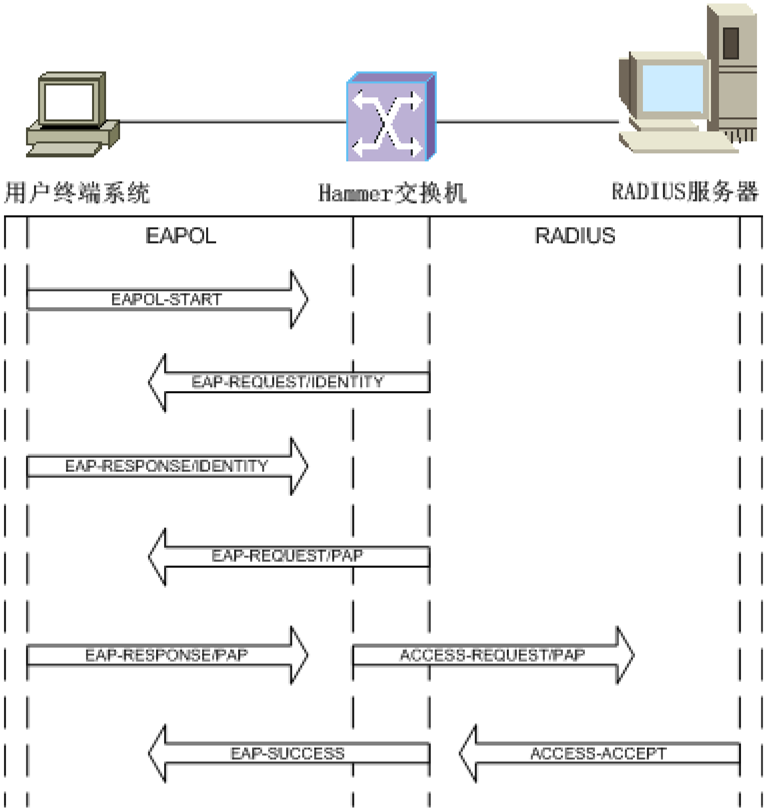


图 9-1 使用 PAP 方式进行身份验证的过程

2．使用 CHAP 方式进行身份验证

如图 9-2 所示，首先用户终端向 Hammer 交换机发送 EAPOL-START 报文请求接入服务，交换机返回 EAP-REQUEST/IDENTITY 报文到用户终端，要求用户提供身份标识，用户终端回复 EAP-RESPONSE/IDENTITY 表示连接建立。然后交换机生成 Challenge 信息，并发送 EAP-REQUEST/CHALLENGE 报文通知用户使用 CHAP 方式验证身份，用户终端返回 EAP-RESPONSE/MD5-CHALLENGE 响应报文给交换机。交换机根据来自用户终端的 EAP-RESPONSE/MD5-CHALLENGE 报文组装并发送 ACCESS REQUEST 报文送到 RADIUS 服务器。RADIUS 服务器对用户进行认证，如果认证通过，返回 ACCESS ACCEPT 报文给交换机，由交换机完成相应操作以允许用户接入，同时发送 EAP-SUCCESS 报文到用户终端通知用户接入成功。

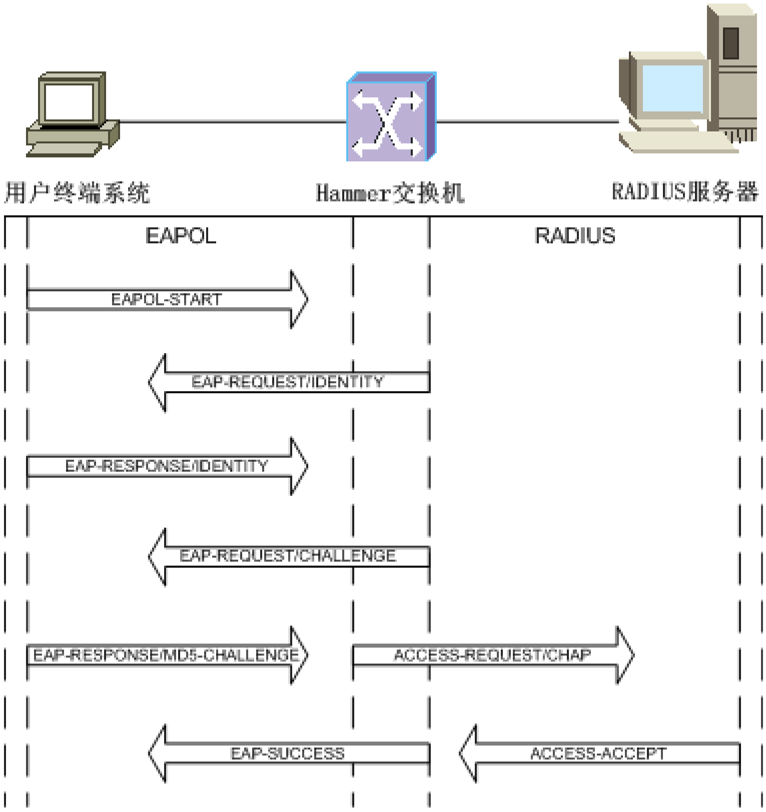


图 9-2 使用 CHAP 方式进行身份验证的过程

3．使用 EAP-MD5 方式进行身份验证

如图 9-3 所示，首先用户终端向 Hammer 交换机发送 EAPOL-START 报文请求接入服务，交换机返回 EAP-REQUEST/IDENTITY 报文到用户终端，要求用户提供身份标识，用户终端回复 EAP-RESPONSE/IDENTITY 表示连接建立。然后由交换机发送 ACCESS-REQUEST 到 RADIUS 服务器，RADIUS 服务器生成 Challenge 信息，并将 ACCESS-CHALLENGE 报文发送给交换机。接下来，交换机向用户终端发送 EAP-REQUEST/CHALLENGE 报文通知用户使用 EAP-MD5 方式验证身份，终端返回 EAP-RESPONSE/MD5-CHALLENGE 报文作为响应。交换机将来自用户终端的 EAP-RESPONSE/MD5-CHALLENGE 报文封装到 ACCESS REQUEST 报文中，并发送到 RADIUS 服务器。RADIUS 服务器对用户进行认证，如果认证通过，则返回 ACCESS ACCEPT 报文给交换机，由交换机完成相应操作以允许用户接入，同时发送 EAP-SUCCESS 报文到用户终端通知用户接入成功。

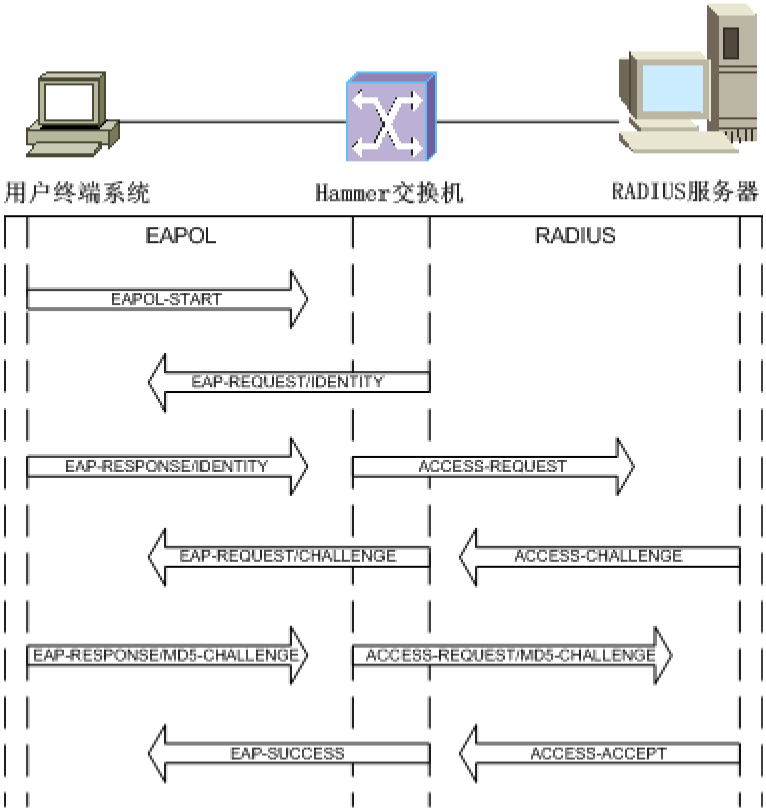


图 9-3 使用 EAP-MD5 方式进行身份验证的过程

9.2 802.1x 协议

在 IEEE 802 所定义的局域网环境中，只要存在物理的连接口，未经授权的网络设备就可以直接或通过连接到局域网的设备进入局域网络。随着局域网技术的广泛应用，在很多网络环境中，往往不希望未经授权的设备或用户连接到网络，使用网络提供的资源和服务。特别是在运营网络中的应用，对其安全认证的要求已经提到了议事日程上。如何既能够利用局域网技术简单、廉价的组网特点，同时又能够对用户或设备访问网络的合法性提供认证，是目前业界讨论的焦点。IEEE 802.1x 协议正是在这样的背景下提出的。

IEEE 802.1x 称为基于端口的访问控制协议（Port Based Network Access Control Protocol），该协议在利用 IEEE 802 LAN 的优势基础上提供了对连接到局域网的设备或用户进行认证和授权的一种手段。通过此方式的认证，能够在 LAN 这种多点访问环境中提供一种点对点识别用户的方式。这里的端口是指连接到 LAN 的一个单点结构，可以是被认证系统的 MAC 地址，也可以是服务器或网络设备上连接 LAN 的物理端口，或者是在 IEEE 802.11 无线 LAN 环境中定义的工作站和访问点。

9.2.1 802.1x 体系结构

IEEE 802.1x 协议的体系结构包括三个重要的组成部分：Supplicant 客户端、Authenticator System 认证系统、Authentication Server 认证服务器。下图描述了三者之间的关系以及相互之间的通信。

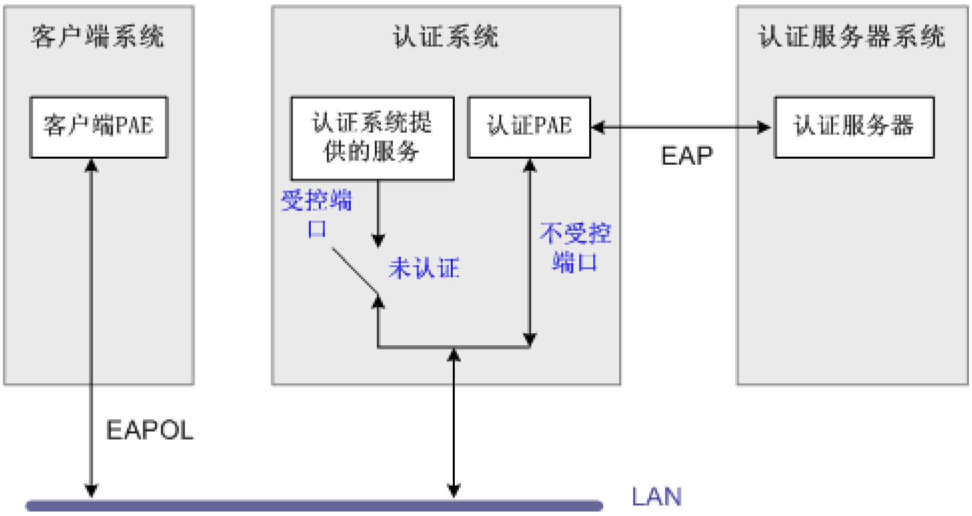


图 9-4 IEEE 802.1x 认证体系结构

客户端系统一般指用户终端系统，该终端系统通常需要安装一个客户端软件，用户通过启动这个客户端软件发起 802.1x 协议的认证过程。为了支持基于端口的接入控制，客户端系统需支持 EAPOL（Extensible Authentication Protocol Over LAN）协议。

认证系统通常指那些支持 802.1x 协议的网络设备，如港湾网络有限公司的 Hammer 系列交换机和无线访问点设备。支持 802.1x 协议的网络设备对应不同的用户端口（可以是物理端口，也可以是用户设备的 MAC 地址）有两个逻辑端口：受控端口（Controlled Port）和不受控端口（Uncontrolled Port）。不受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，可保证客户端始终能够发出或接受认证。受控端口只有在认证通过的状态下才可打开，用于传递网络资源和服务。受控端口可配置为双向受控、仅输入受控两种方式，以适应不同的应用环境。如果用户未通过认证，则受控端口处于未认证状态，用户无法访问认证系统提供的服务。图 9-4 中认证系统的受控端口处于未认证状态，因此客户端无法访问认证系统提供的服务。

PAE 是端口访问实体（Port Access Entity），分为客户端 PAE 和认证系统 PAE：

- 客户端PAE：位于客户端，主要负责响应来自认证系统建立信任关系的请求。
- 认证系统PAE：位于认证系统，负责与客户端的通信，把从客户端收到的信息传送给认证服务器以完成认证。

认证系统的 PAE 通过不受控端口与客户端 PAE 进行通信，二者之间运行 EAPOL 协议。认证系统的 PAE 与认证服务器之间运行 RADIUS（Remote Authentication Dial In User Service）协议。

认证系统和认证服务器之间的通信可以通过网络进行，也可以使用其他的通信通道。例如当认证系统和认证服务器集成在一起时，两个实体之间的通信就可以不采用 RADIUS 协议。

认证服务器通常为 RADIUS 服务器，该服务器可以存储有关用户的信息，比如用户所属的 VLAN、CAR 参数、优先级、用户的访问控制列表等等。当用户通过认证后，认证服务器会把用户的相关信息传递给认证系统，由认证系统构建动态的访问控制列表，用户的后续流量将接受上述参数的监管。

图 9-4 描述了终端用户的认证机制，对于网络设备之间的认证也是一样。例如：当一个网络设备 A 要求访问网络设备 B 所提供的服务时，系统 A 的 PAE 就成为客户端（Suppliant），系统 B

的 PAE 为认证系统（Authenticator）；如果 B 要求访问 A 所提供的服务时，B 的 PAE 就成为客户端，A 的 PAE 就成为认证系统。

9.2.2 802.1x 认证机制

802.1x 作为一种认证协议，在实现的过程中有很多重要的工作机制，这里我们主要介绍其中四种机制：

- 认证发起机制
- 退出认证机制
- 重新认证机制
- 认证报文丢失重传机制

1．认证发起机制

认证过程可以由用户主动发起，也可以由认证系统发起。一方面当认证系统探测到有未经过认证的用户使用网络时，就会主动发起认证,另一方面客户端可以通过客户端软件向认证系统发送 EAPOL-Start 报文发起认证。

◎ 由认证系统发起的认证

当认证系统检测到有未经认证的用户使用网络时，就会发起认证。在认证开始之前，端口的状态被强制 “ 未认证 ”。

如果客户端的身份标识不可知，则认证系统会发送 EAP-Request/Identity 报文，请求客户端发送身份标识。这样，就开始了典型的认证过程。

客户端在收到来自认证系统的 EAP-Request/Identity 报文后，将发送 EAP-Response/Identity 报文响应认证系统的请求。

认证系统支持定期的重新认证，可以随时对一个端口发起重新认证的过程。如果端口状态为已认证状态，则当认证系统发起重新认证时，该端口通过认证，状态保持不变；如果未通过认证，则端口的状态改变为未认证状态。

◎ 由客户端发起认证

如果用户要上网，则可以通过客户端软件向认证系统发送 EAPOL-Start 报文主动发起认证。认证系统在收到客户端发送的 EAPOL-Start 报文后，会发送 EAP-Request/Identity 报文响应用户请求，要求用户发送身份标识，这样就启动了一个认证过程。

2．退出认证机制

有以下几种方式可以造成认证系统把端口状态从已认证状态改变成未认证状态：

a) 客户端未通过认证服务器的认证；

b) 管理性的控制端口始终处于未认证状态；

c) 与端口对应的 MAC 地址出现故障（管理性禁止或硬件故障）；

d) 客户端与认证系统之间的连接失败，造成认证超时；

e) 重新认证超时；

f) 客户端未响应认证系统发起的认证请求；

g) 客户端发送 EAPOL-Logoff 报文，主动下线。

退出已认证状态的直接结果就是导致用户下线，如果用户要继续使用网络则要重新发起一个认证过程。为什么要专门提供一个 EAPOL-Logoff 机制呢？主要是出于如下的安全考虑：当一个用户从一台终端退出后，很可能其他用户不通过发起一个新的认证过程，就可以利用该设备访问网络。提供专门的退出机制，以确保用户与认证系统专有的会话进程被中止，可以防止用户的访问权限被他人盗用。通过发送 EAPOL-Logoff 报文，可以使认证系统将对应的端口状态改变为未认证状态。

3．重新认证机制

为了保证用户和认证系统之间的链路处于激活状态，而不因为用户端设备发生故障造成异常死机，从而影响对用户计费的准确性，认证系统可以定期发起重新认证过程，该过程对于用户是透明的，即用户无需再次输入用户名和密码。

重新认证由认证系统发起，时间是从最近一次成功认证后算起。交换机上的重新认证功能可以激活或关闭，默认情况下是关闭的。重新认证的时间间隔默认值为 3600 秒（一个小时）。

注意：

重新认证的时间设定需要认真的规划，认证系统对端口进入的 MAC 地址的检测能力会影响到该时间的设定。如果对 MAC 地址的检测比较可靠，则重新认证时间可以设长一些。

4．认证报文丢失重传机制

对于认证系统和客户端之间通信的 EAP 报文，如果发生丢失，由认证系统负责进行报文的重传。在设定重传的时间时，考虑网络的实际环境，通常会认为认证系统和客户端之间报文丢失的几率比较低以及传送延迟低，因此一般通过一个超时计数器来设定，默认重传时间为 30 秒钟。

由于对用户身份合法性的认证最终由认证服务器执行，认证系统和认证服务器之间的报文丢失重传也很重要。

另外注意，对于用户的认证，在执行 802.1x 认证时，只有认证通过后，才能由 DHCP 发起（如果配置为 DHCP 的自动获取）和 IP 地址分配的过程。当客户终端配置了 DHCP 自动获取 IP 地址时，则可能在未启动 802.1x 客户端之前，就发起了 DHCP 的请求，而此时认证系统处于禁止通行状态，这样认证系统会丢掉 DHCP 请求帧。

9.2.3 协议实现内容

802.1x 协议在实现整个安全认证的过程中，其三个关键部分（客户端、认证系统、认证服务器）之间是通过不同的通信协议进行交互的，因此有必要对其相关的通信协议做一介绍。

EAP 协议

802.1x 协议采用 EAP 协议在客户端、认证系统和认证服务器之间进行通信。EAP（Extensible Authentication Protocol 扩展的认证协议，RFC 2284）是 PPP 认证的一个通用协议，支持多种认证机制。EAP 在链路控制（LCP）阶段并不选择好一种认证机制，而是把这一步推迟到认证阶段，这就允许认证系统在确定某种特定认证机制之前请求更多的信息。

通过支持 EAP 协议，认证系统只需控制其受控端口的状态，而并不干涉通过非受控端口在客户端和认证服务器之间传递的认证信息，这样可实现认证流和业务流的完全分离。可以使用认证服务器来实现各种认证机制，认证系统仅仅需要传送认证信息，并根据认证返回的结果控制受控端口的状态。

EAP 帧结构如图 9-5 所示：

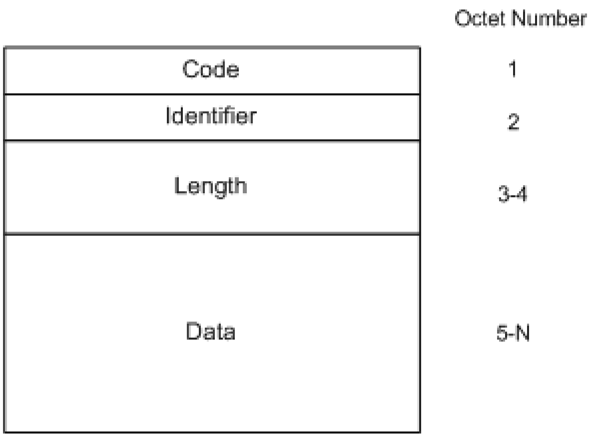


图 9-5 EAP 帧结构

EAP 帧格式中各字段含义如下：

字段	占用字节数	描述
Code	1 个字节	表示 EAP 帧的四种类型： 1. Request 2. Response 3. Success 4. Failure
Identifier	1 个字节	用于匹配 Request 和 Response。Identifier 的值和系统端口一起单独标识一个认证过程
Length	2 个字节	表示 EAP 帧的总长度
Data	0 或更多字节	表示 EAP 数据

EAPOL 协议

802.1x 协议定义了一种报文封装格式，这种报文称为 EAPOL（EAP over LANs 局域网上的扩展认证协议）报文，主要用于在客户端和认证系统之间传送 EAP 协议报文，以允许 EAP 协议报文在 LAN 上传送。

EAPOL 帧结构如图 9-6 所示：

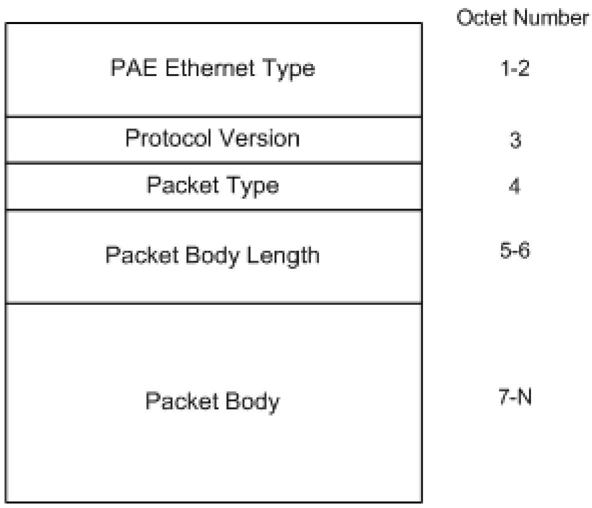


图 9-6 EAPOL 帧结构

EAPOL 帧格式中各字段含义如下：

字段	占用字节数	描述
PAE Ethernet Type	2 个字节	表示协议类型，802.1x 分配的协议类型为 888E
Protocol Version	1 个字节	表示 EAPOL 帧的发送方所支持的协议版本号。本规范使用值为 0000 0001
Packet Type	1 个字节	表示传送的帧类型，如下几种帧类型： a) EAP-Packet. 值为 0000 0000 ，表示为 EAP 帧 b) EAPOL-Start.值为 0000 0001 ，表示为 EAPOL-Start 帧 c) EAPOL-Logoff. 值为 0000 0010，表示为 EAPOL-Logoff 请求帧 d) EAPOL-Key.值为 0000 0011 ，表示为 EAPOL-Key 帧. e) EAPOL-Encapsulated-ASF-Alert. 值为 0000 0100
Packet Body Length	2 个字节	表示 Packet Body 的长度
Packet Body	0 或更多字节	如果 Packet Type 为 EAP-Packet、EAPOL-Key 或 EAPOL-Encapsulated-ASF-Alert 的值，则 Packet Body 取相应的值；对于其他帧类型，该值为空。

EAPOL 帧可以携带 802.1q 的 VLAN 标记。

EAPOL 帧在二层传送时，必须要有目标 MAC 地址，当客户端和认证系统彼此之间不知道发

送的目标时，其目标 MAC 地址使用由 802.1x 协议分配的组播地址 01-80-c2-00-00-03。

9.2.4 与不支持 802.1x 的设备的兼容

对于从一个没有认证的系统过渡到认证系统，最理想的状态是希望能够平滑的进行过渡。由于 802.1x 协议是一个比较新的协议，如果应用在原有的旧网络中，则可能存在与不支持 802.1x 协议的设备的兼容性问题。

如果客户端支持 802.1x 协议，而网络设备不支持（也就是没有认证系统），则客户端是不会收到认证系统响应的 EAP-Request/Identity 报文。在 802.1x 认证发起阶段，客户端首先发送 EAPOL-Start 报文到 802.1x 协议组申请的组播 MAC 地址，以查询网络上可以处理 802.1x 的设备（即认证系统），由于网络中没有设备充当认证系统，所以客户端是得不到响应的。因此客户端在发起多次连接请求无响应后，自动认为已经通过认证。

如果客户端不支持 802.1x 协议，而网络中存在 802.1x 协议的认证系统，则客户端是不会响应认证系统发送的 EAP-Request/Identity 报文，因此端口会始终处于未认证状态。在这种情况下，客户端只能根据协议参数 OperControlledDirections 设定的值通过受控端口访问认证系统，通过未受控端口访问某些通过设置可以访问的服务。

9.3 RADIUS 认证技术

RADIUS 的全称为（Remote Access Dail-In User Service），它是对远程拨号用户访问进行认证的一种协议，是在 RADIUS Server 和 RADIUS Client 之间进行认证、授权、计费的协议标准。认证即辨别用户是谁的过程，通常该过程通过输入有效的用户名和密码实现；授权是指对完成认证过程的用户授予相应权限，解决他能做什么的问题，在一些身份认证的实现中，认证和授权是统一在一起的；计费（Accounting）则是统计用户做过什么的过程，包括用户使用的时间和费用，可通过用户占用系统的时间、接收和发送的信息量来衡量。

RADIUS 采用 Client/Server 模型，在 NAS 上运行的是 Client 端，负责将用户信息传送到指定的 RADIUS 服务器上，并根据服务器返回的结果进行相应的处理。RADIUS 服务器包括两种类型：授权认证服务器和计费服务器。授权认证服务器（RADIUS Authentication Server）负责接收用户的连接请求、验证用户身份，并返回给客户需要的相关配置信息。一个授权认证服务器也可以作为 RADIUS 客户的代理，将其连接到另一个授权认证服务器。计费服务器（RADIUS Accounting Server）负责接受用户计费开始请求和计费结束请求，并实现计费功能。

RADIUS 具有以下属性：

- RADIUS以Client/Server模式工作，实现了对远程用户的身份认证、授权和计费功能。
- RADIUS Client主要用来将用户信息传递给RADIUS Server；Server则对用户进行认证，并返回用户的配置信息。
- 为保证传输的安全性，RADIUS报文携带由MD5算法求得的128位验证字。
- 认证具有灵活性。采取多种认证机制，包括PAP和CHAP。

提示：本版本无计费功能。

接入服务配置命令详解

9.4 802.1x 配置命令

9.4.1 打开/关闭 802.1x 认证功能.

【命令语法】config dot1x [enable|disable]

【参数说明】

参数	说明
enable	打开 802.1x 认证功能
disable	关闭 802.1x 认证功能

【使用指导】如果端口 25 和 26 没有设置为强制认证状态，则执行此命令的结果会导致端口 25 和 26 的 Learning 功能开关自动设为 disable，因此当此命令是在 Telnet 中执行时，会导致 Telnet 死掉。（此种情况建议先设定端口 25 和 26 为强制已认证状态。）

【配置实例】打开 802.1x 认证功能

Harbour(config)# config dot1x enable

9.4.2 打开/关闭用户绑定功能.

【命令语法】config dot1x binduser [enable|disable]

【参数说明】

参数	说明
enable	打开用户绑定功能
disable	关闭用户绑定功能

【配置实例】打开用户绑定功能

Harbour(config)# config dot1x binduser enable

9.4.3 添加/删除端口绑定的用户

【命令语法】config dot1x binduser [add|delete] port [<portlist>|all] user <username>

【参数说明】

参数	说明
add|delete	添加/删除
portlist	端口列表
all	所有端口
username	操作对象的名称

【配置实例】在 24 端口增加绑定用户 3100_test

Harbour(config)# config dot1x binduser add port 24 user 3100_test

9.4.4 清除用户绑定

【命令语法】config dot1x binduser clear-all

【配置实例】清除用户绑定信息

Harbour(config)# config dot1x binduser clear-all

9.4.5 清除 802.1x 的统计信息

【命令语法】config dot1x clear-statistic

【配置实例】清除 802.1x 的统计信息

Harbour(config)# config dot1x clear-statistic

9.4.6 打开/关闭 Keepalive 功能

【命令语法】config dot1x keepalive [enable|disable]

【参数说明】

参数	说明
enable	打开 Keepalive 功能
disable	关闭 Keepalive 功能

【配置实例】打开 Keepalive 功能

Harbour(config)# config dot1x keepalive enable

9.4.7 设置 Keepalive 机制

【命令语法】config dot1x keepalive mechanism [ping-pong|state-machine]

【参数说明】

参数	说明
ping-pong	采用 ping-pong 检测机制
state-machine	采用状态机检测机制

【配置实例】采用状态机检测机制

Harbour(config)# config dot1x keepalive mechanism state-machine

9.4.8 设置 Keepalive 的阈值 max-no-respone-count

【命令语法】config dot1x keepalive max-no-response-count <2-30>

【参数说明】

参数	说明
2-30	次数边界值，最少 2 次，最多 30 次，默认值为 5

【配置实例】设置 max-no-response-count 的次数值为 3

Harbour(config)# config dot1x keeapalive max-no-response-count 3

9.4.9 设置 Keepalive 的阈值 ping-pong-period

【命令语法】config dot1x keepalive ping-pong-period <60-600>

【参数说明】

参数	说明
60-600	ping-pong 方式的周期，时间区间为 60 到 600 秒，默认值 120 秒

【配置实例】设置发起 ping-pong 检测的周期为 300 秒

Harbour(config)# config dot1x keepalive ping-pong-period 300

9.4.10 设置 Keepalive 的阈值 state-machine-period

【命令语法】config dot1x keepalive state-machine-period <10-3600>

【参数说明】

参数	说明
10-3600	state machine 方式的检测周期值，时间区间为 10 到 3600 秒，默认值为 300 秒

【配置实例】设置 state machine 检测的周期为 400 秒

Harbour(config)# config dot1x keepalive state-machine-period 400

9.4.11 底层交换绑定

【命令语法】config dot1x low-level-switch-bind [enable|disable]

【参数说明】

参数	说明
enable	打开底层交换绑定
disable	关闭底层交换绑定

【配置实例】打开底层交换绑定

Harbour(config)# config dot1x low-level-switch-bind enable

9.4.12 重发数据的最大次数

【命令语法】config dot1x max-req <1-10>

【参数说明】

参数	说明
1-10	重发数据的次数，最多 10 次，最少 1 次，默认值为 2

【配置实例】设置数据重发次数为 3

Harbour(config)# config dot1x max-req 3

9.4.13 多用户绑定到同一端口

【命令语法】config dot1x multiple-host-one-port max-host-count <2-128>

【参数说明】

参数	说明
2-128	一个端口可以绑定的用户数目，默认值为 10

【配置实例】设置端口绑定用户数目为 9

Harbour(config)# config dot1x multiple-host-one-port max-host-count 9

9.4.14 通过命令行强制用户下线

【命令语法】config dot1x pae force-logoff all

【配置实例】强制所有用户下线

Harbour(config)# config dot1x pae force-logoff all

9.4.15 通过命令行强制特定的 PAE id 客户端下线

【命令语法】config dot1x pae force-logoff id <paeid>

【参数说明】

参数	说明
paeid	客户端的 paeid

【配置实例】强制 paeid 为 1 的客户端下线

Harbour(config)# config dot1x pae force-logoff id 1

9.4.16 通过命令行强制某端口的所有用户下线

【命令语法】config dot1x pae force-logoff port <portno>

【参数说明】

参数	说明
portno	端口号，强制端口<portno>下的所有用户退出认证状态

【配置实例】强制端口 16 下的所有用户退出认证状态

Harbour(config)# config dot1x pae force-logoff port 16

9.4.17 通过命令行强制某个 MAC 的用户下线

【命令形式】: config dot1x pae force-logoff mac <address> {port <portno>}*1

【参数说明】

参数	说明
address	MAC 地址
port <portno>	端口参数

【应用实例】：强制 MAC 地址为 00-05-3b-51-02-92 的用户退出认证状态

Harbour(config)# config dot1x pae force-logoff mac 00053b510292

9.4.18 配置 quiet-period

【命令语法】config dot1x quiet-period <0-65535>

【参数说明】

参数	说明
0-65535	时间间隔的范围，单位秒，默认值为 60 秒

【配置实例】配置 quiet-period 为 30 秒

Harbour(config)# config dot1x quiet-period 30

9.4.19 打开/关闭重认证功能

【命令语法】config dot1x re-authentication [enable|disable]

【参数说明】

参数	说明
enable	打开认证功能
disable	关闭 802.1x 认证功能

【配置实例】打开 802.1x 重认证功能

Harbour(config)# config dot1x re-authentication enable

9.4.20 配置重认证周期

【命令语法】config dot1x re-authentication period <1-65535>

【参数说明】

参数	说明
1-65535	重认证的周期，单位秒，默认值为 3600 秒

【配置实例】配置重人证周期为 10800 秒

Harbour(config)# config dot1x re-authentication period 10800

9.4.21 配置最大重认证次数

【命令语法】config dot1x reauth-max <1-10>

【参数说明】

参数	说明
1-10	欲设置的重认证的次数，默认值为 2

【配置实例】配置重认证的最大次数为 3

Harbour(config)# config dot1x reauth-max 3

9.4.22 配置服务器超时期限

【命令语法】config dot1x server-timeout <1-65535>

【参数说明】

参数	说明
1-65535	超时时间阈值，单位秒，默认值 30 秒

【配置实例】配置超时时间为 20 秒

Harbour(config)# config dot1x server-timeout 20

9.4.23 配置客户端超时期限

【命令语法】config dot1x supp-timeout <1-65535>

【参数说明】

参数	说明
1-65535	超时时间阈值，单位秒，默认值 30 秒

【配置实例】配置客户端超时时间阈值为 25 秒

Harbour(config)# config dot1x supp-timeout 25

9.4.24 配置认证系统向客户端系统重传 EAP-Request/Identity 数据帧的时间间隔

【命令语法】config dot1x tx-period <1-65535>

【参数说明】

参数	说明
1-65535	重传数据帧的时间间隔，单位秒，默认值 30 秒

【配置实例】配置重传数据帧的时间间隔为 20 秒

Harbour(config)# config dot1x tx-period 20

9.4.25 配置端口的认证状态

【命令语法】config port [<portlist>|all] dot1x authcontrolledportcontrol [auto|forceauth|forceunauth]

【参数说明】

参数	说明
<portlist>|all	表示对[某个|所有]端口的操作
auto|forceauth|forceunauth	表示端口的状态，默认值为 auto

【配置实例】配置端口 25,26 为 forceauth 状态.

Harbour(config)# config port 25-26 dot1x authcontrolledportcontrol forceauth

9.5 802.1x 显示命令

有关 802.1x 的显示命令如表 9-1 所示。

表 9-1： 802.1x 显示命令列表

显示命令	描述
show dot1x	显示 802.1x 功能开启或关闭的状态以及相关的参数配置信息
show dot1x binduser port [<portlist>|all]	显示端口上的用户绑定信息
show dot1x binduser status	显示绑定开关的状态
show dot1x binduser user <username>	显示某一用户名的绑定信息
show dot1x low-level-switch-bind	显示底层绑定开关状态
show dot1x pae all	显示所有 PAE 的信息
show dot1x pae id <id>	显示某个 PAE ID 的信息
show dot1x pae mac <address> {port <portno>}*1	根据 MAC 显示与之相关联的 PAE 信息
show dot1x pae port <portno>	根据端口号显示与之相关联的所有创建的 PAE 信息，以及 PAE 总数
show dot1x statistic	显示 802.1x 统计信息
show port [<portlist>|all] dot1x	显示一组端口对应的 802.1x 相关信息，包括端口号、当前创建的 PAE 实体的个数以及在某一时刻曾经创建过最多的 PAE 实体的个数
show 802.1x	显示 802.1x Forwarding 的配置信息

9.6 配置 RADIUS 认证服务

认证服务器（Authentication Server）具有如下属性：

- 认证服务器通过ID号进行标识。NAS包含一个认证服务器列表，当NAS发送认证请求时，它从列表中选择最先添加的且处于可用状态的认证服务器，或者选择由用户指定的认证服务器。因此在配置某个认证服务器时，必须将该服务器加入到列表中，如果不再使用某个认证服务器了，可以将它从列表中删除。
- 添加新的认证服务器时，如果指定的ID号在服务器列表中已经存在，若仍要在新的认证服务器上使用这个ID，需要先删除使用该ID的认证服务器，然后再加入新的认证服务器。
- server-ip是认证服务器的IP地址。
- client-ip是RADIUS Client的IP地址，即交换机上连接认证服务器的端口所对应的IP地址。

- udp-port端口号，RADIUS Server 和RADIUS Client通过UDP发送数据包，对于认证服务器而言，这个端口号默认为1812。

9.6.1 启用 RADIUS 认证功能

【命令语法】radius authentication enable

【配置实例】启用 RADIUS 认证功能

Harbour(config)# radius authentication enable

9.6.2 禁用 RADIUS 认证功能

【命令语法】radius authentication disable

【配置实例】禁用 RADIUS 认证功能

Harbour(config)# radius authentication disable

9.6.3 配置 RADIUS Server 和 RADIUS Client

【命令语法】radius authentication add-server id <0-4> server-ip <A.B.C.D> client-ip <A.B.C.D> {udp-port <1-6500>}*1

【参数说明】

参数	说明
id <0-4>	交换机标识的 RADIUS Server 的编号
server-ip <A.B.C.D>	RADIUS Server 的 IP 地址
client-ip <A.B.C.D>	RADIUS Client 的 IP 地址
udp-port <1-6500>	RADIUS 认证端口号，默认值为 1812

【配置实例】添加 RADIUS Server id=0, server-ip 192.168.88.111, client-ip: 192.168.88.66, UDP 端口号 1812

Harbour(config)# radius authentication add-server id 0 server-ip 192.168.88.111 client-ip 192.168.88.66 udp-port 1812

9.6.4 配置共享秘钥

【命令语法】radius authentication config-server id <0-4> shared-secret <secret>

【参数说明】

参数	说明
id <0-4>	交换机上标识 Server 的 id 号
secret	共享秘钥

【配置实例】配置 server id = 0 的共享秘钥为 harbour

Harbour(config)# radius authentication config-server id 0 shared-secret harbour

9.6.5 配置最大重传次数

【命令语法】radius authentication config-server id <0-4> max-retransmit-count <2-10>

【参数说明】

参数	说明
id <0-4>	server id 的标识符
2-10	最大重传的次数，默认值为 3 次

【配置实例】对于配置的 RADIUS Server 0，配置最大重传的次数为 2

Harbour(config)# radius authentication config-server id 0 max-retransmit-count 2

9.6.6 配置最大重传丢弃数

【命令语法】radius authentication config-server id <0-4> max-retransmit-drop-count <2-30>

【参数说明】

参数	说明
id <0-4>	server id 的标识符
2-30	最大重传丢弃次数，默认值为 3 次

【配置实例】对于配置的 RADIUS Server 0，配置最大重传丢弃次数为 2

Harbour(config)# radius authentication config-server id 0 max-retransmit-drop-count 2

注意：该参数用于判断是否断掉 RADIUS Server。当在规定的重传次数内没有收到 Server 的响应，则记录一次丢弃。

9.6.7 配置最大失败数

【命令语法】radius authentication config-server id <0-4> max-send-fail-count <2-30>

【参数说明】

参数	说明
id <0-4>	server id 的标识符
2-30	最大重传失败次数，默认值为 3 次

【配置实例】对于配置的 RADIUS Server 0，配置最大重传失败次数为 2

Harbour(config)# radius authentication config-server id 0 max-send-fail-drop-count 2

注意:该参数用于判断是否断掉 RADIUS Server。当最大丢弃数达到最大失败数时，则断掉 RADIUS Server。

9.6.8 配置重发时间间隔

【命令语法】radius authentication config-server id <0-4> retransmit-interval <5-300>

【参数说明】

参数	说明
id <0-4>	server id 的标识符
5-300	重传时间间隔，默认值为 10 次

【配置实例】对于配置的 RADIUS Server 0，配置重发时间间隔为 15

Harbour(config)# radius authentication config-server id 0 retransmit-interval 15

9.6.9 配置 Server 的状态为 active

【命令语法】radius authentication config-server id <0-4> status active

【参数说明】

参数	说明
id <0-4>	server id 的标识符

【配置实例】配置 Server 的状态为 active

Harbour(config)# radius authentication config-server id 0 status active

9.6.10 删除配置的 Server

【命令语法】radius authentication delete-server id <0-4>

【参数说明】

参数	说明
id <0-4>	server id 的标识符

【配置实例】删除配置的 server 0

Harbour(config)# radius authentication delete-server id 0

9.7 RADIUS 显示命令

有关 RADIUS 信息的显示命令见表 9-2。

表 9-2 RADIUS 显示命令列表

show radius idpool	显示 RADIUS 已经配置的 ID Pool 中的信息
show radius {configuration}*1	显示 RADIUS 的当前配置信息

第10章 日志模块(Syslog)配置

本章主要包括以下内容：

- 日志模块概述
- 日志功能基本配置
- 日志信息存储方式配置
- 日志信息显示方式配置
- 查看日志模块的配置情况
- 日志模块命令列表

10.1 日志模块概述

日志模块主要用来记录整个系统的运行情况以及用户操作行为。完整的日志模块能够帮助管理员及时了解和监控系统的工作情况，并实时记录系统的异常信息。日志信息来源于系统中所有的运行模块，日志系统完成信息的收集、管理、存储和显示。日志信息可以显示到终端 Monitor，这种方式主要用于调试和查看系统状态。也可以存储到日志服务器，这种方式用于长期跟踪系统的运行情况以及用户的命令行操作行为。

10.2 日志功能基本配置

10.2.1 打开或关闭日志服务

【命令作用】打开或关闭日志服务功能

【命令语法】config syslog [enable|disable]

【参数说明】

参数	说明
enable	表示打开日志服务功能
disable	表示关闭日志服务功能

【命令模式】配置模式

【使用指导】只在配置模式下使用该命令。

【配置实例】打开日志服务功能。

```
Harbour(config)# config syslog enable
```

Successfully changed syslog service to enable

10.2.2 配置所要记录的日志信息的类型

【命令语法】config syslog type [<name>|all] [enable|disable]

【参数说明】

参数	说明
name	系统中支持的日志类型
all	所有日志类型
enable	表示对指定类型的信息进行记录
disable	表示不记录

【命令模式】配置模式

【使用指导】可用 show syslog configuration 来查看日志类型，目前支持的类型有：AUTH，BGP，CLI，SYSLOG，DEVCTRL，ARP，DOT1X，NAS，OSPF，PORT，FDB，RADIUS，RIP，ROUTE，SNMP，STP，SYSTEM，VLAN，WEB，SERVICE，DHCPR，VDSLDRV 等。

【配置实例】

Harbour(config)# config syslog type auth enable

Successfully changed syslog type auth to enable.

注册 AUTH 类型的日志信息，日志模块将对 AUTH 类型的日志信息进行记录。

10.2.3 配置所要记录的日志信息的最低级别

【命令作用】配置日志模块对某一级别和某一级别以上的日志信息进行记录

【命令语法】config syslog lowest-level <0-7>

【参数说明】

参数	说明
<0-7>	目前支持的日志信息级别，从 0 到 7 依次为 EMERG，ALERT，CRITERR，WARNING，NOTICE，INFO，DEBUG

【命令模式】配置模式

【配置实例】

Harbour(config)# config syslog lowest-level 3

Successfully changed syslog service lowest-lever level 3 [ERR].

级别 3 和级别 3 以上的日志信息将被记录。

10.2.4 打开命令行操作日志记录功能

【命令作用】配置日志模块是否对命令行操作行为进行日志记录

【命令语法】record command-line [enable|disable]

【参数说明】

参数	说明
enable	表示对命令行操作进行记录
disable	表示对命令行操作不进行记录

【命令模式】配置模式

【使用指导】命令行操作的日志信息级别为 6，即 INFO 类型。

【配置实例】

Harbour(config)# record command-line enable

Successfully changed syslog record CLI to enable.

允许对命令行操作行为记录日志信息。

10.3 日志信息存储方式配置

10.3.1 打开或关闭日志信息保存到日志服务器的功能

【命令作用】配置日志模块是否保存日志信息到日志服务器

【命令语法】config syslog server [enable|disable]

【参数说明】

参数	说明
enable	表示保存日志信息到服务器
disable	表示不保存日志信息到服务器

【命令模式】配置模式

【使用指导】在配置之前，保证日志服务器服务程序已启动。

【配置实例】

Harbour(config)# config syslog server enable

Successfully changed syslog service logto server enable.

Warning: Syslog server config is empty.Please add syslog server.

允许日志保存到日志服务器。

10.3.2 增加或删除一个日志服务器

【命令作用】增加或删除一个日志服务器，包括配置日志服务器的 IP 地址，服务端口，日志信息的级别等信息

【命令语法】config syslog [add|delete] server <A.B.C.D>

{[port] <1-65535>}*1 {[facility] <0-7>}*1

【参数说明】

参数	说明
add	表示增加一个日志服务器
delete	表示删除一个日志服务器
A.B.C.D	表示日志服务器的 IP 地址
port	日志服务器上接收日志进程的服务端口号
[facility] <0-7>	对应于日志信息的级别,就是说这个日志服务器将保存某个级别和某个级别以上的日志信息

【命令模式】配置模式

【使用指导】可以使用一条命令配置日志服务器信息，也可以使用多条子命令进行配置。关于日志服务器服务程序的配置详见相关手册。

【配置实例】

Harbour(config)# config syslog add server 10.12.3.4 port 8808 facility 5

Successfully added syslog server 10.12.3.4.

配置了一个 IP 地址为 10.12.3.4 的日志服务器，服务端口为 8808，日志信息的级别为 5。

Harbour(config)# config syslog delete server 10.1.4.1 port 6500 facility 1

Successfully deleted syslog server 10.1.4.1

删除了一个日志服务器，其 IP 地址为 10.1.4.1，服务端口为 6500，优先级为 1。

10.4 日志信息显示方式配置

10.4.1 打开或关闭终端显示日志信息的功能

【命令作用】配置日志信息是否输出到用户终端

【命令语法】config syslog monitor-terminal [enable|disable]

【参数说明】

参数	说明
enable	表示允许日志信息输出到客户端
disable	表示不允许日志信息输出到客户端

【命令模式】配置模式

【使用指导】该命令是服务命令，将对所有终端起作用。

【配置实例】

Harbour(config)# config syslog monitor-terminal enable

Successfully changed syslog service logto monitor-terminal to enable.

允许日志信息输出到所有用户终端。

10.4.2 打开或关闭在本终端显示日志信息的功能

【命令作用】决定是否在本终端输出日志信息

【命令语法】monitor [on|off]

【参数说明】

参数	说明
on	表示允许在本终端输出日志信息
off	表示不允许在本终端输出日志信息

【命令模式】配置模式

【使用指导】该命令只对本终端起作用。

【配置实例】

Harbour(config)# monitor on

Successfully changed your terminal display syslog messages.

允许日志信息输出到自己的终端。

10.4.3 配置是否显示时间信息

【命令作用】决定是否在本终端输出时间信息

【命令语法】monitor display timestamp [none|time|datetime]

【参数说明】

参数	说明
none	不显示时间和日期
time	只显示时间，不显示日期
datetime	时间日期都显示

【命令模式】配置模式

【使用指导】该命令主要用来决定是否在本终端输出时间信息。

【配置实例】在本终端输出时间信息。

Harbour(config)# monitor timestamp datetime

10.4.4 配置在终端可以显示的日志信息的最低级别

【命令作用】决定在本终端输出某一级别和某一级别以上的日志信息

【命令语法】monitor display lowest-level <0-7>

【参数说明】

参数	说明
<0-7>	目前支持的日志信息级别,从 0 到 7 依次为 EMERG ，ALERT ，CRITERR， WARNING，NOTICE，INFO， DEBUG

【命令模式】配置模式

【使用指导】该命令只对本终端起作用。

【配置实例】

Harbour(config)# monitor display lowest-level 3

Successfully changed monitor lowest-lever level 3 [ERR]。

将在本终端输出级别 3 和级别 3 以上类型的日志信息。

10.4.5 配置在终端可以显示的日志信息的类型

【命令作用】决定在本终端输出某一类型的日志信息

【命令语法】monitor display type [<typename>|all] [on|off]

【参数说明】

参数	说明
typename	系统中支持的日志类型
all	所有日志类型

【命令模式】配置模式

【使用指导】该命令只对本终端起作用，可用 show syslog configuration 来查看日志类型，目前支持的类型有：AUTH，BGP，CLI，SYSLOG，DEVCTRL，ARP，DOT1X，NAS，OSPF，PORT，FDB，RADIUS，RIP，ROUTE，SNMP，STP，SYSTEM，VLAN，WEB，SERVICE，DHCPR,VDSLDRV 等。

【配置实例】

Harbour(config)# monitor display type all on

Successfully changed to display all messages.

将在本终端输出所有类型的日志信息。

10.5 查看日志模块的配置情况

10.5.1 查看整个日志模块的配置信息

【命令作用】显示日志模块的所有配置信息，包括各种服务的打开和关闭情况等。

【命令语法】show syslog {configuration}*1

【命令模式】配置模式

【使用指导】可以列出日志模块的所有配置信息，对使用日志模块命令具有一定指导作用。

【配置实例】

Harbour(config)# show syslog configuration

Syslog Service is up.

--Service Syslog logto flashfile is up.

--Service Syslog logto server is down.

Have no syslog server.

--Service Syslog logto monitor-terminal is up.

--Log messages that not lower than level 4 [WARNING].

--Log these types messages:

--Not log these types messages:

:AUTH:BGP:CLI:SYSLOG:DEVCTRL:ARP:DOT1X:NAS:OSPF:PORT:FDB:RADIUS:RIP:ROUTE:SNMP:STP:SYSTEM:VLAN:WEB:SERVICE:DHCPR:VDSLDRV

Record command-line is disabled

10.5.2 查看对本终端的日志显示属性的配置情况

【命令作用】包括所配置的可以在本终端显示的日志类型，日志级别以及时间信息等。

【命令语法】show monitor {configuration}*1

【命令模式】配置模式

【使用指导】该命令只对本终端起作用。

【配置实例】

Harbour(config)# show monitor configuration

Monitor has been on.

Monitor show messages with none timestamp.

Monitor only display log messages that not lower than level 7 [DEBUG].

Monitor display messages of these types:

Monitor donot display messages of these types:

AUTH:BGP:CLI:SYSLOG:DEVCTRL:ARP:DOT1X:NAS:OSPF:PORT:FDB:RADIUS:RIP:ROUTE:SNMP:ST

P:SYSTEM:VLAN:WEB:SERVICE:DHCPR:

10.6 日志模块命令列表

日志模块命令列表

<table>
<tr><th>命令</th><th>描述</th></tr>
<tr><td>config syslog [enable|disable]</td><td>启用或禁用日志服务功能。enable 表示启用，disable 表示禁用。</td></tr>
<tr><td>config syslog monitor-terminal [enable|disable]</td><td>允许或禁止把日志信息输出到终端。enable 表示允许，disable 表示禁止。</td></tr>
<tr><td>config syslog lowest-level <0-7></td><td>配置所要记录的日志信息的最低级别。表示系统将对等于或大于 lowest-level 的日志类型做日志信息。0:系统不可用，1：实时操作，2：严重，3:错误， 4:告警，5: 提示，6: 一般信息， 7：调试</td></tr>
<tr><td>config syslog type [<name>|all] [enable|disable]</td><td>启用或禁用某一个日志类型或所有日志类型的日志功能。name 为该日志类型名字，all 表示代表所有日志类型。enable 表示启用，disable 表示禁用。</td></tr>
<tr><td>record command-line [enable|disable]</td><td>是否对命令行操作做日志记录。enable 表示允许，disable 表示禁止。</td></tr>
<tr><td>config syslog server [enable|disable]</td><td>允许或禁止把日志信息输出到日志服务器。enable 表示允许，disable 表示禁止。</td></tr>
<tr><td>config syslog [add|delete] server <A.B.C.D> {[port] <1-65535>}*1 {[facility] <0-7>}*1</td><td>配置或删除一个日志服务器。<A.B.C.D>为 IP 地址，port 为端口，facility 为优先级别。</td></tr>
<tr><td>show syslog {configuration}*1</td><td>显示日志模块所有配置信息。</td></tr>
<tr><td>monitor [on|off]</td><td>开始显示或结束日志信息输出到本终端。</td></tr>
<tr><td>monitor display timestamp [none|time|datetime]</td><td>允许在本终端输出时间信息。</td></tr>
<tr><td>monitor display lowest-level <0-7></td><td>设置本终端所要输出的日志信息的级别。该命令执行后，在本终端只显示等于或大于该级别的日志信息。</td></tr>
<tr><td>monitor display type [<typename>|all] [on|off]</td><td>设置哪些日志类型的的日志信息可以输出到本终端。</td></tr>
<tr><td>show monitor {configuration}*1</td><td>显示对日志信息输出到本终端的配置信息。</td></tr>
</table>

注意：

在检测 VDSL 端口 SYNC 或者 LINK 状态改变的 Syslog 时，只有当状态改变的间隔超过某个时间间隔（大约 5 秒到 10 秒，间隔的长短取决于系统的繁忙程度），才会有 Syslog 发出。

第11章 利用 Web 管理 Hammer3100 系列交换机

HammerOS 还提供了利用 Web 来管理并配置交换机的功能，其主要功能有：登录时的身份验证，对设备进行管理，维护并配置系统信息，修改并保存配置信息以及退出登录操作。通过这些 Web 功能模块，您就可以非常直观地配置交换机的各项参数。

11.1 登录

HammerOS 是港湾网络有限公司为 Hammer 系列交换机开发的操作系统，可以运行在 μHammer、FlexHammer、BigHammer 交换机及 Hammer3100 系列交换机上。同时也提供了 Web 功能，用户可以利用 Web 来完成对交换机的配置管理工作。

11.1.1 登录 Web 界面

登录 Web 界面按以下步骤进行：

1．在配置模式，利用命令：

【命令语法】config ipaddress <A.B.C.D> <A.B.C.D>

【参数说明】

参数	说明
<A.B.C.D>	前面<A.B.C.D>为配置给交换机的 IP 地址，后面<A.B.C.D>为该 IP 地址的子网掩码

或者利用命令：

【命令语法】config ipaddress <A.B.C.D/M>

【参数说明】

参数	说明
A.B.C.D	配置给交换机的 IP 地址
M	子网掩码长度

【配置实例】配置交换机的 IP 地址为 10.1.17.111，键入命令：

Harbour(config)#config ipaddress 10.1.17.111 255.0.0.0

或者，键入命令：

Harbour(config)#config ipaddress 10.1.17.111/8

2.在配置模式下，利用命令：

Harbour(config)#service webserver enable

以确保 Web 服务处于打开状态。可以用 show service 命令查看其状态。

3．在 Web 浏览器中输入交换机缺省配置的 IP 地址，并按回车后，您将看到如图 11-1 所示界面:



图 11-1　初始界面

如图 11-1 所示，您可以选择中文或英文界面。例如：我们选择中文，您将看到如图 11-2 所示界面：



图 11-2 HammerOS 欢迎界面

HammerOS 中提供了两种用户权限，即管理员用户权限和普通用户权限。相应的对 HammerOS 来说就有两种模式，只读模式和配置模式。在只读模式下，用户只能对系统信息进行读操作，而不能进行修改配置信息的操作。但在配置模式下，用户可以对交换机信息进行各种系统配置。以普通用户身份登录的用户只能进入只读模式，而不能进入配置模式，只有以系统管理员身份登录的用户才能进入配置模式。

11.1.2 登录身份

系统缺省内置了一个用户帐号，用户名是 admin，在用户名中输入帐号，在登录密码中输入用户密码，缺省密码是 harbour。此用户是管理员。缺省用户 admin 的帐号不能被删除，用户也不能被修改，只能修改他的密码。如果用户选择登录身份是系统管理员还需要在管理密码栏中输入密码。输入完毕之后点“ **登录** ”按钮，即可登录，如果输入错误可点按钮“ **清除** ”重新输入。

如图 11-3 为例， 我们以系统管理员身份登录：



图 11-3 登录界面

单击“登录”后，如图 11-4 所示：



图 11-4 设备管理

此时我们就可以以管理员的身份通过 Web 对交换机进行管理配置了。如果输入的登录信息有错误，则出现图 11-5：



图 11-5 登录错误界面

此时需要重新输入登录系统信息。

11.1.3 基于 Web 的功能管理介绍

如图 11-4 所示，该 Web 功能管理包含以下模块：

- 设备管理
- 用户管理
- 系统信息
- 保存配置
- 退出登录

系统默认初始界面是设备管理，如图 11-4 所示。

11.2 IP 地址管理

在以系统管理员身份登录交换机之后，点击设备管理一栏中的“ **IP 地址** ”，如图 11-6

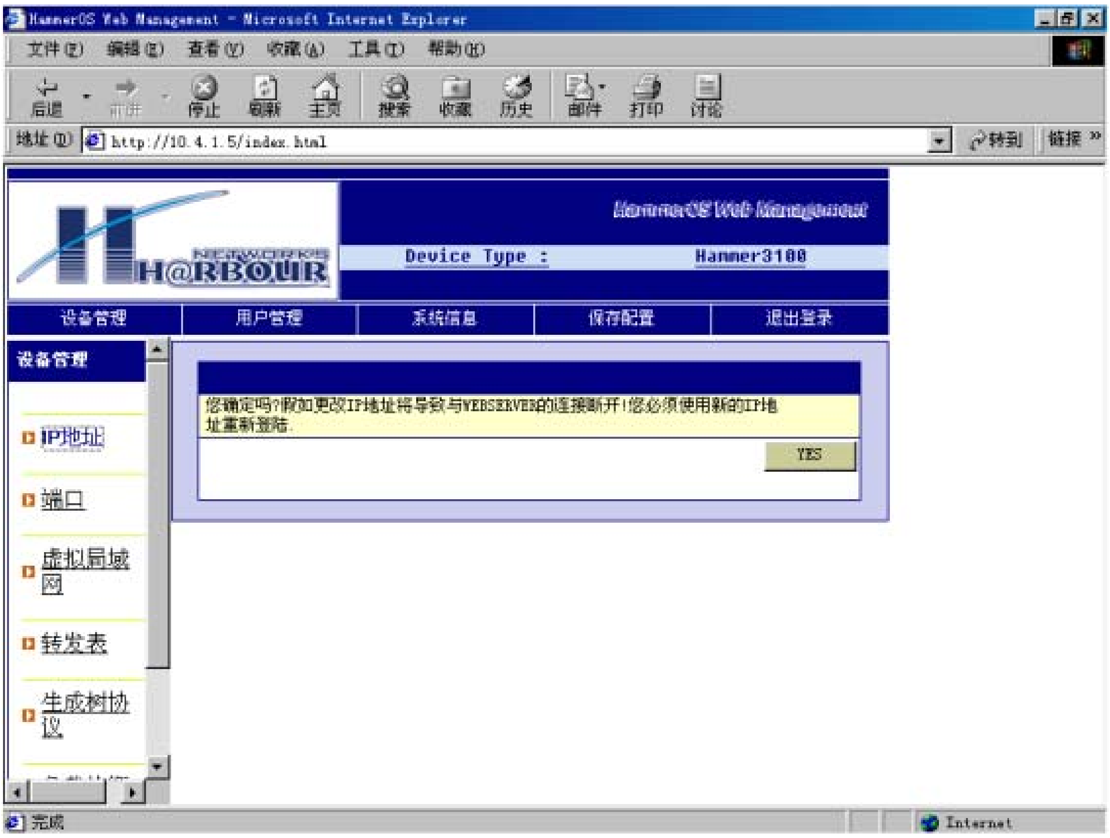


图 11-6 IP 地址管理 1

如果确实想更改 IP 地址，那么点击“ **YES** ”按钮，如图 11-7 所示

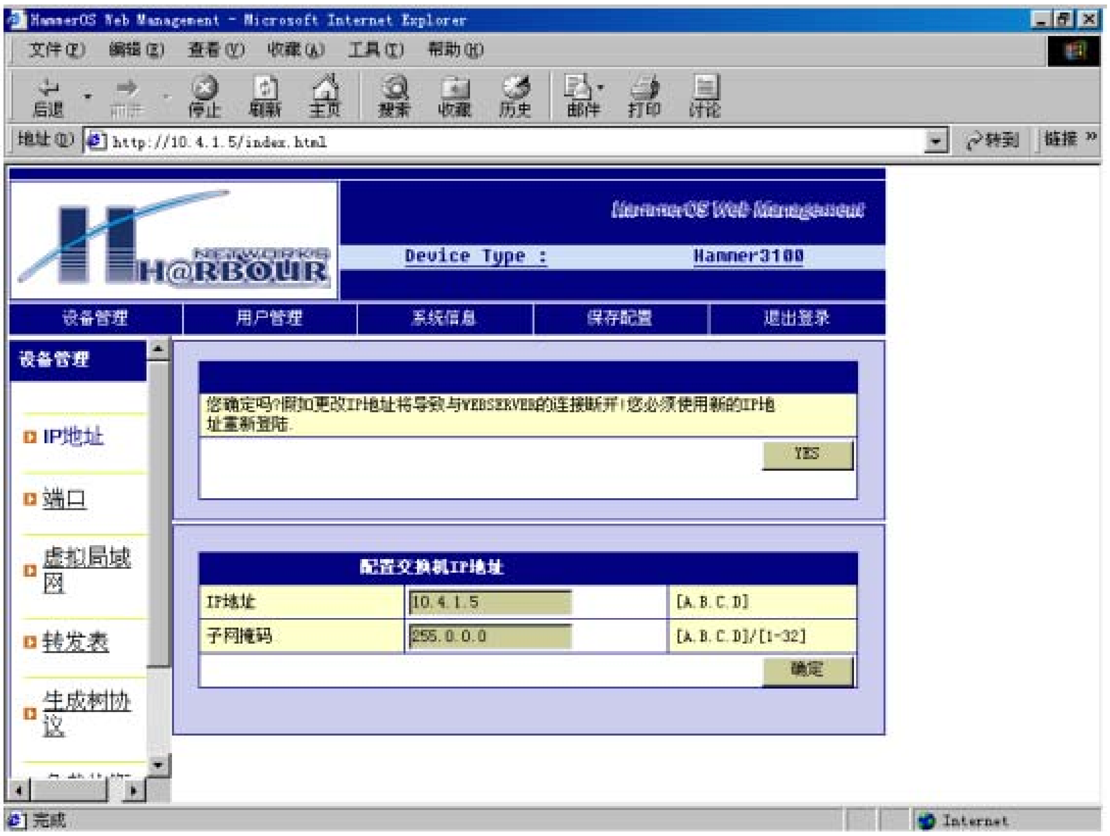


图 11-7 IP 地址管理 2

输入您要配置的 IP 地址和子网掩码，点击“ **确定** ”按钮，就可以完成对交换机的 IP 地址配置。

11.3 端口配置

HammerOS 可以对端口进行以下几种配置：

- 打开或关闭指定端口
- 打开或关闭指定端口的自适应功能
- 配置端口速度
- 配置端口的半双工或全双工模式
- 配置端口的流控
- 配置端口的MAC地址学习

在设备管理模块下，又可以划分为对 IP 地址的配置，对端口的配置，对虚拟局域网的配置，对转发表的配置，对生成树协议的配置，对负载均衡的配置，对镜像端口信息的配置。

在成功登录 Web Server 之后选择屏幕上面菜单栏的设备管理，再单击左侧设备管理下的“ 端口 ”，可以看到图 11-4 所示的界面。(该交换机面板显示了当前的端口状态)：

- 绿色表示该端口当前是打开状态并且链路已连接
- 红色表示该端口当前是打开状态但无链路连接
- 深黄色表示该端口当前是关闭状态

如果想要对端口进行配置，单击面板上的相应端口就会有相应的表格显示，如图 11-8 为端口 9 的配置信息，并且可以在此表格中对该端口进行配置，包括：

- 管理状态
- 自适应
- 双工
- 速率
- 流控
- MAC学习

几种属性的设置，选择您所需要的配置后单击“ **应用修改** ”按钮即可，如图 11-8 所示：



图 11-8 端口管理 1

除此之外还能够显示端口其他的一些属性，比如：属于哪个虚拟子网，属于哪个负载均衡组，属于哪个生成树协议域， 统计的信息等等。通过单击其它端口可以获取特定端口的相关信息。

注意：

1.在配置时要关闭自适应

2.以上信息通过拉动图 11-8 的滑动条即可

3.其显示信息如图 11-9 所示



图 11-9 端口管理 2

11.4 VLAN 的设置

11.4.1 VLAN 的设置标准

Hammer3100 系列交换机最多支持 32 个 VLAN。用户可以根据以下标准创建 VLAN：

- 物理端口
- 802.1Q tag
- 以上标准的组合

11.4.2 Web 中 VLAN 的管理

在主控制界面左侧设备管理链接栏中单击“ **虚拟局域网** ”进入虚拟局域网控制界面，如图 11-10 所示。

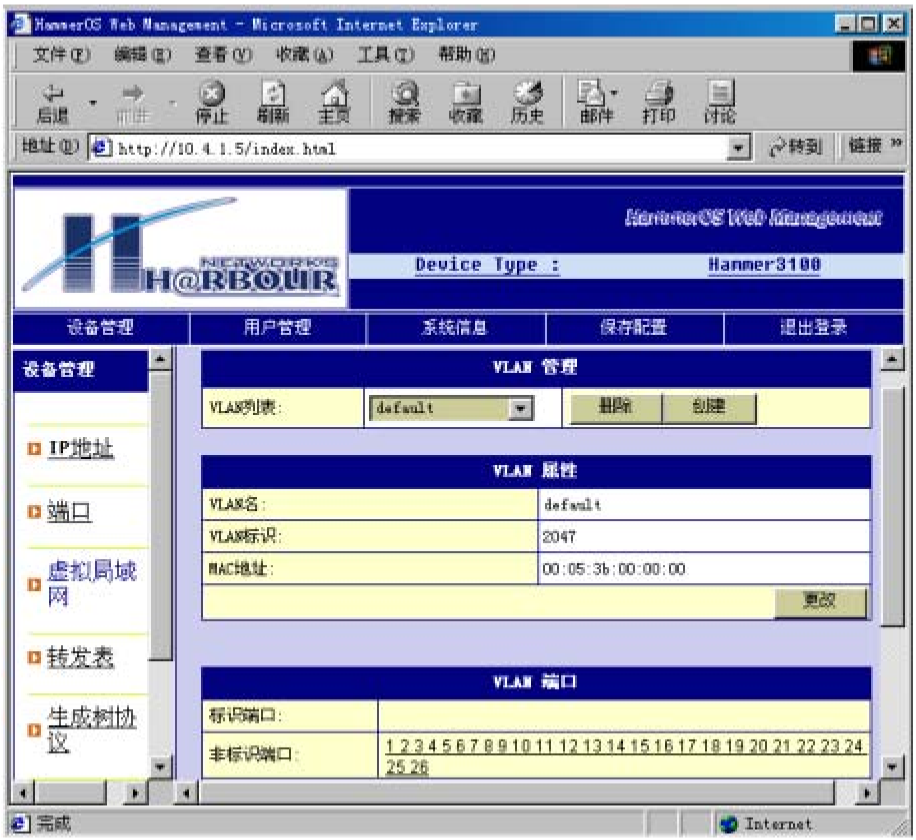


图 11-10 虚拟局域网管理 1

VLAN 端口列表中显示属于该 VLAN 的端口,点击相应的端口将显示该端口的信息。另外，在本 Web 界面中还提供了删除和创建 VLAN、更改特定 VLAN 的属性。

11.4.3 查看 VLAN 的配置情况

在 VLAN 列表的下拉菜单中选择所需要进行操作的 VLAN 名，下面的表格将显示相应 VLAN 的配置情况。如图 11-10 显示的为 VLAN default 的信息。

11.4.4 创建新的 VLAN

点击 “ **VLAN 管理** ” 表格中的 “ **创建** ” 按钮，如图 11-11 所示。

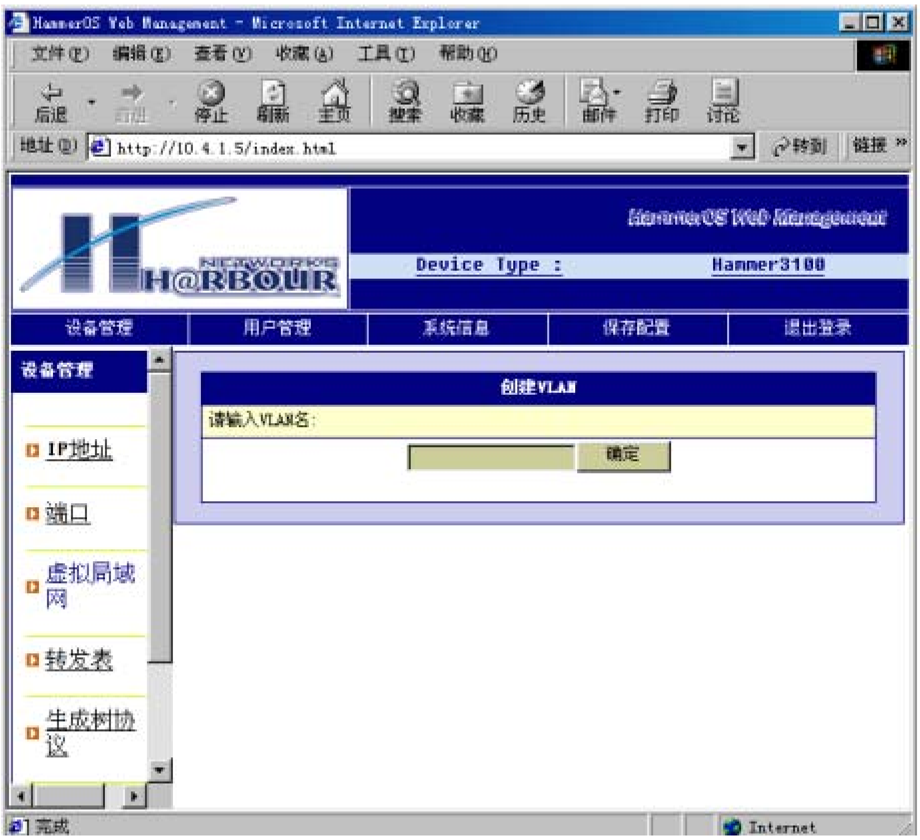


图 11-11 虚拟局域网管理 2

在对话框中输入所要创建的 VLAN 名比如 “ VLAN1 ”，然后点击 “ **确定** ”，结果如图 11-12 所示

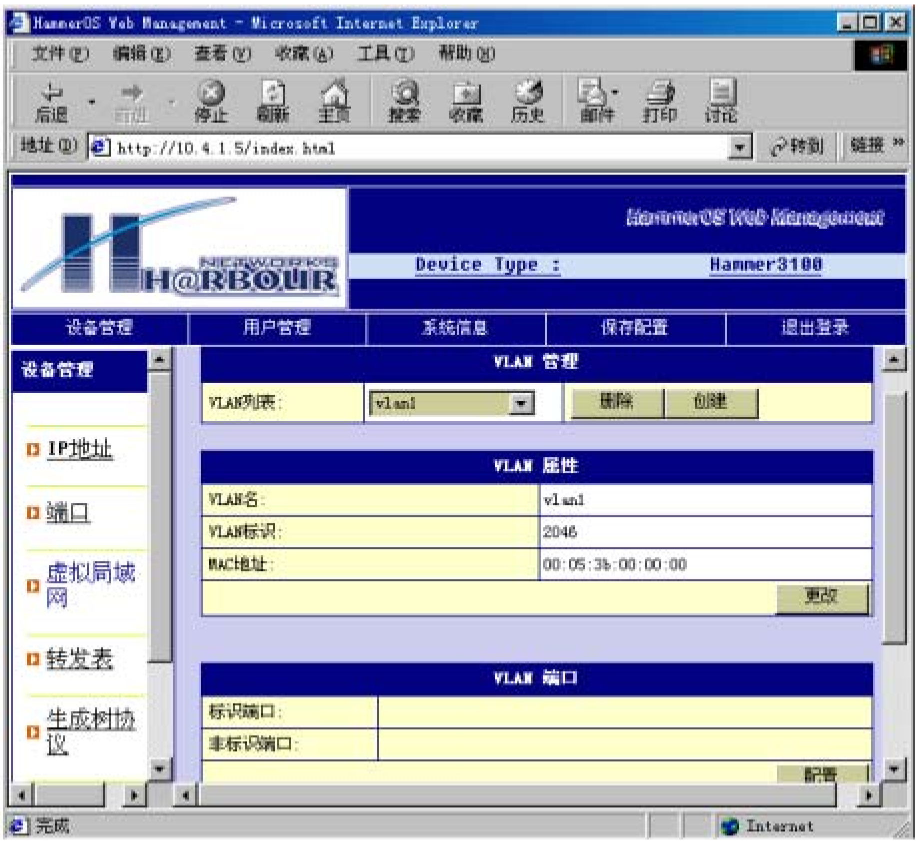


图 11-12 虚拟局域网管理 3

11.4.5 VLAN 信息的修改

在图 11-12 中点击 “ **更改** ” 按钮，出现界面，如图 11-13 所示。

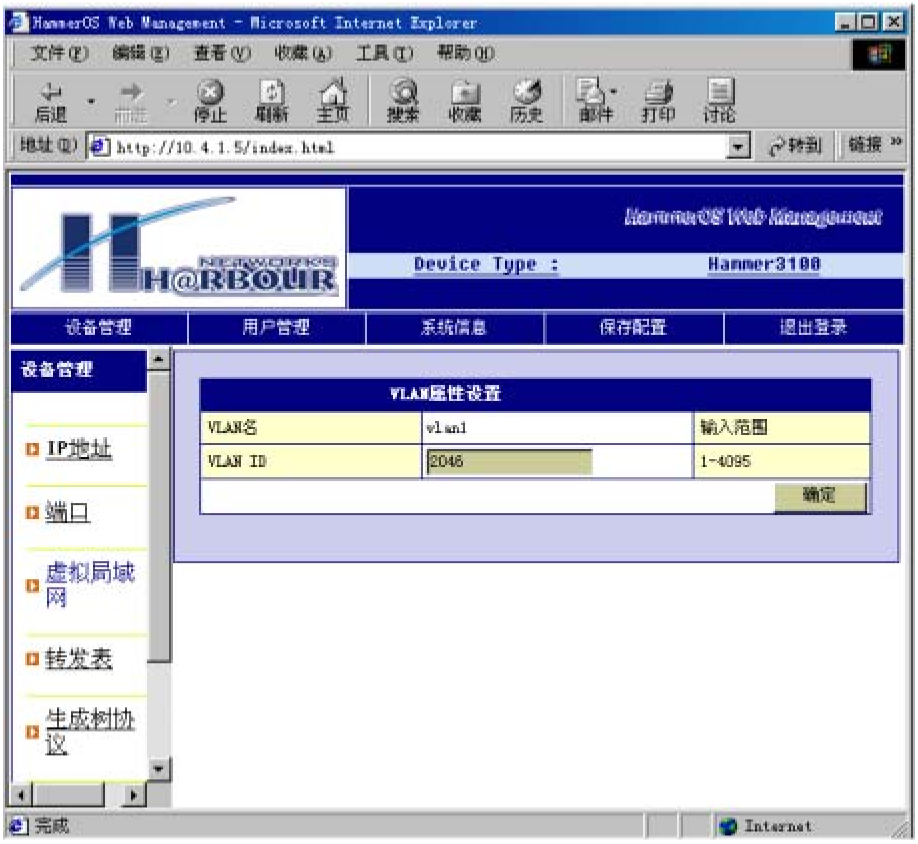


图 11-13 虚拟局域网管理 4

在输入框中输入您所需要配置的数据。例如：VLAN ID 2046

然后单击“ **确定** ”按钮即可。出现如图 11-14 所示界面。

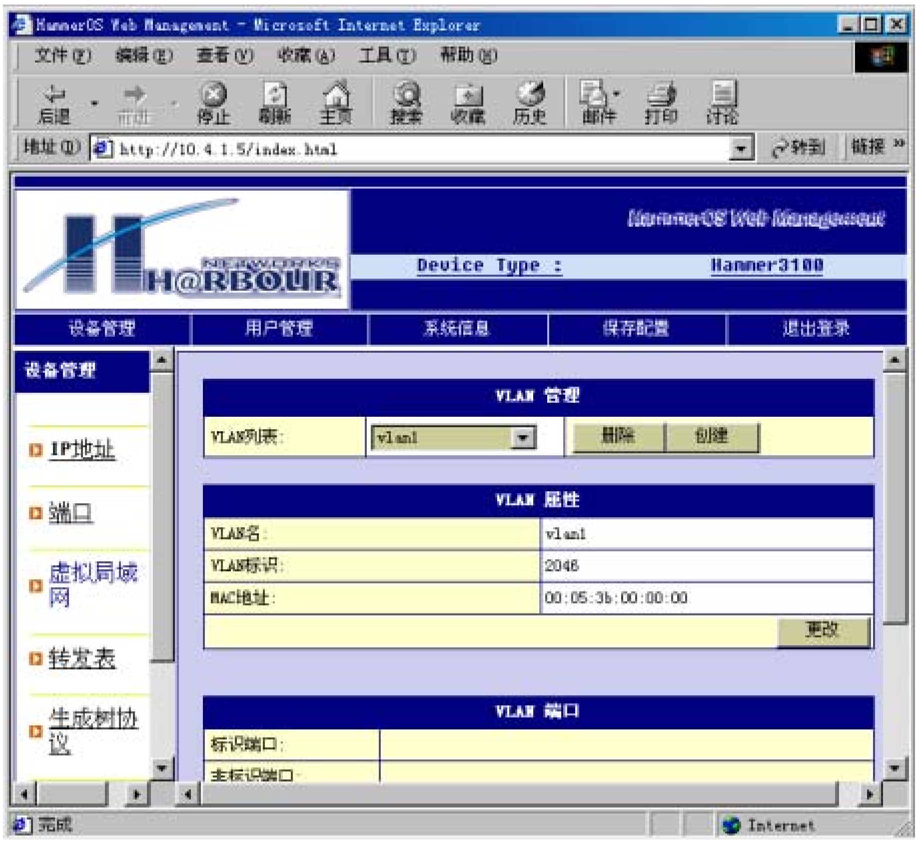


图 11-14 虚拟局域网管理 5

11.4.6 VLAN 的删除

如图 11-14 所示：在 VLAN 列表中选择要进行删除操作的 VLAN 名，然后单击“删除”按钮即可进行删除操作。

11.4.7 VLAN 端口的配置

如图 11-14 所示：单击 VLAN 端口表格中的“配置”按钮进入 VLAN 端口配置界面如图 11-15 所示：

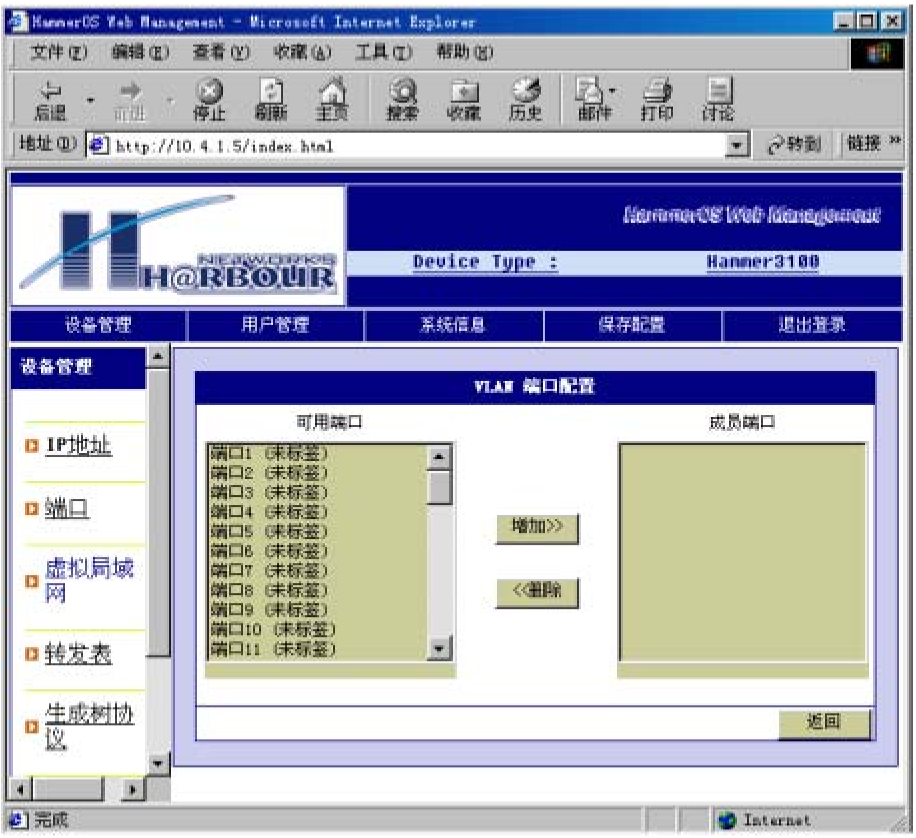


图 11-15 虚拟局域网管理 6

在左边的可用端口框中显示了可以选择的端口（包括 tagged 和 untagged 的端口）。

- 您选择所需要加入的端口后单击“ **增加** ”按钮；
- 如果需要删除VLAN中的端口则在成员框中选择要操作的端口，然后单击“ **删除** ”按钮即可；
- 当一切操作结束之后，单击“ **返回** ”按钮返回VLAN的控制界面。

11.4.8 配置 VLAN 的 inputport 来改变 VLAN 中端口的 defaultVID

如图 11-14 所示：单击 INPUTPORT 表格中的“ **配置** ”按钮进入 INPUTPORT 配置界面，如图 11-16 所示：

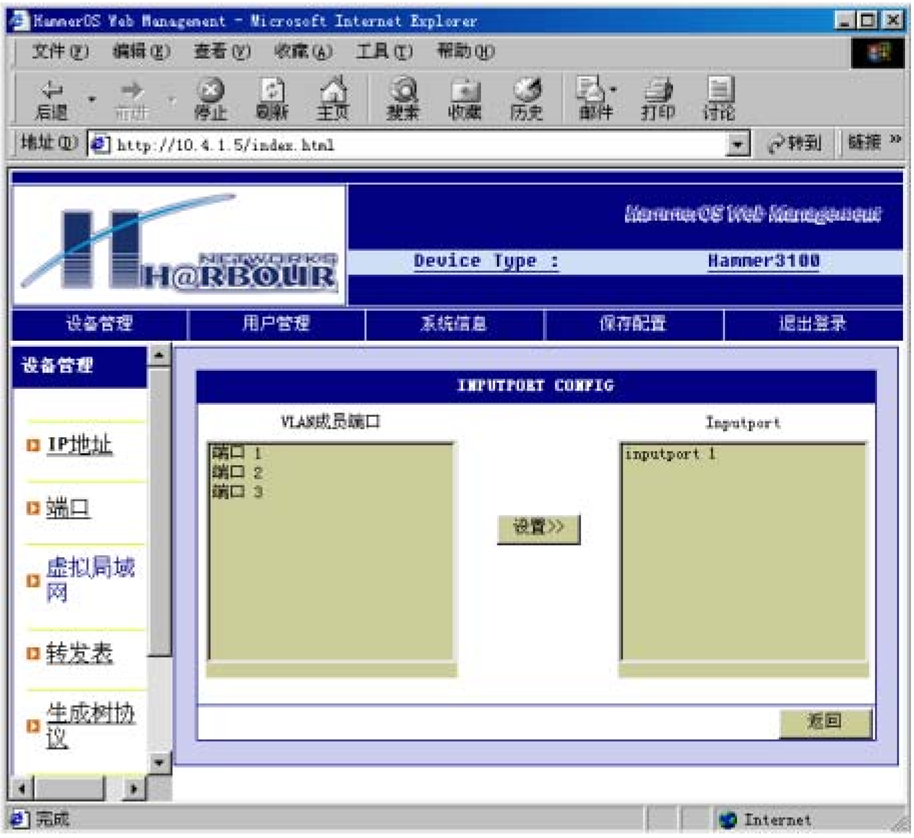


图 11-16 虚拟局域网管理 7

在左边的 VLAN 成员端口框中显示了可以选择的端口：

- 您选择所需要加入的端口后单击“**设置**”按钮；
- 当一切操作结束之后，单击“**返回**”按钮返回VLAN的控制界面。

11.4.9 错误处理

假如我们修改 VLAN default 的信息，比如删除 default VLAN 时，系统就会报错，错误界面如图 11-17 所示：



图 11-17 错误返回界面

这时我们单击“**返回**”即可恢复。

11.5 FDB 地址表的配置

本节主要讲述如何在 HammerOS Web Management 上配置 FDB 地址表。在 Hammer3100 系列交换机中，通过 Web Management 可以增加地址表项到 FDB 地址表中。从而实现对各种数据包的处理，即根据数据包的源地址和目的地址来决定该数据是过滤还是转发。

11.5.1 通过 Web 配置 FDB 地址表

首先点击设备管理下的“**转发表**”出现图 11-18。配置 FDB 地址表可以参照如下图表所示的信息进行设置。

11.5.2 设置 FDB 地址表中的地址表项老化时间

例如：我们设置地址表老化时间（Agingtime）为 80，如下图所示:



图 11-18 转发表 1

在老化时间处填入 80 后，选择提交按钮即可，如想修改，选择重置按钮，重新输入即可。如果老化时间（Ageingtime）被设置为 0，那么该地址表项将存储在 FDB 地址表中而不会被动态删除，直到交换机关机或者重启。

11.5.3 创建一个永久的地址表项

当创建的 FDB 地址是单播地址时，只可以对应一个端口号

选择不同的 VLAN，PORT 栏将产生与之对应的 Port 端口号列表



图 11-19 转发表 2

选择相应虚拟局域网、端口号，输入 MAC 地址、类型，单击 “ **提交** ” 按钮即可。

11.5.4 显示 FDB 地址表中的地址表项

用如下的查询方式可以浏览 FDB 地址表中的地址表项，查询条件有如下四种：

all: 查询本交换机所有的 FDB 地址表项信息

Permanent: 查询本交换机所有固定的 FDB 地址表项信息

Age: 查询本交换机所有会老化的 FDB 地址表项信息

CPU: 查询本交换机中所有送往 CPU 的 FDB 地址表项信息

例如：浏览形式为 Permanent，点击 “ **提交** ” 按钮，出现如图 11-20 所示画面。



图 11-20 转发表 3

其它查询条件作类似操作。

注意：用户定义的地址表项可以删除，其余项不可删除。

11.5.5 错误处理

如果我们设置老化时间越界，则出现如图 11-21 所示界面。

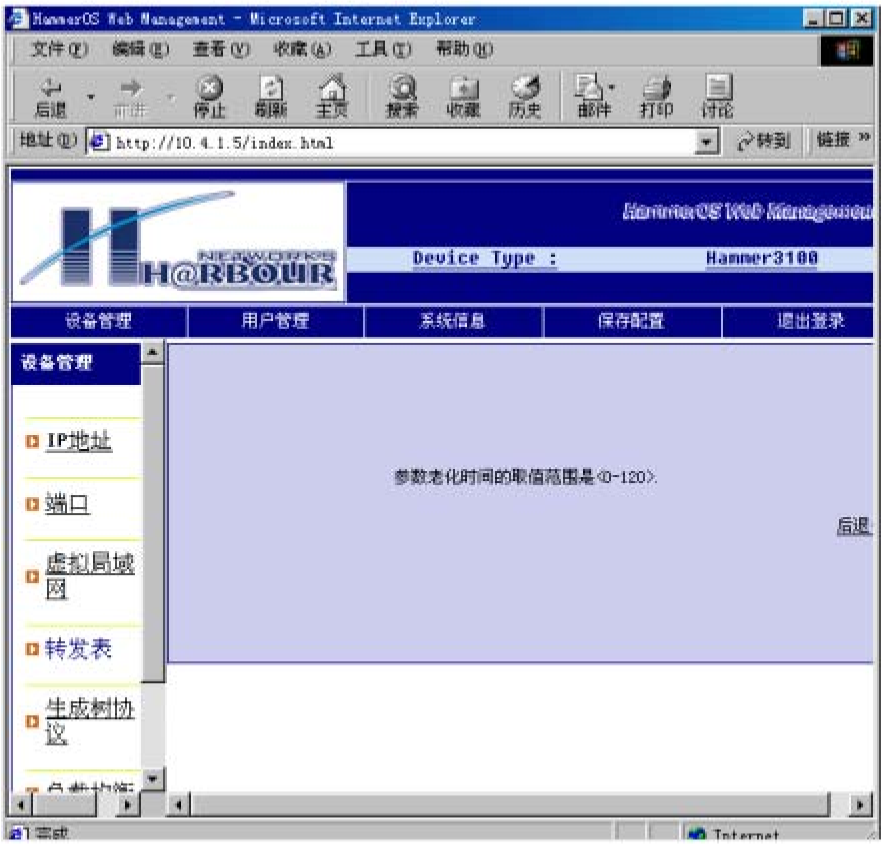


图 11-21 老化时间错误界面

这时点击“后退”即可。

11.6 STP 的配置

11.6.1 配置 STP

配置 STP 需要做如下操作：

- 使能生成树协议域
- 使能参与STP协议计算的端口

一旦运行 STP 协议后，您可能需要根据具体的网络结构调整 STP 协议的一些参数。以下的 STP 协议参数可以在 HammerOS 中调整：

- 优先级
- 桥发送BPDU时间间隔
- 桥切换时间间隔
- 根报文老化最大时间间隔

另外每个端口上有以下参数可以调整：

- 根路径开销
- 优先级

11.6.2 基于 Web 的 STP 配置

可以参照以下图配置 STP 协议；

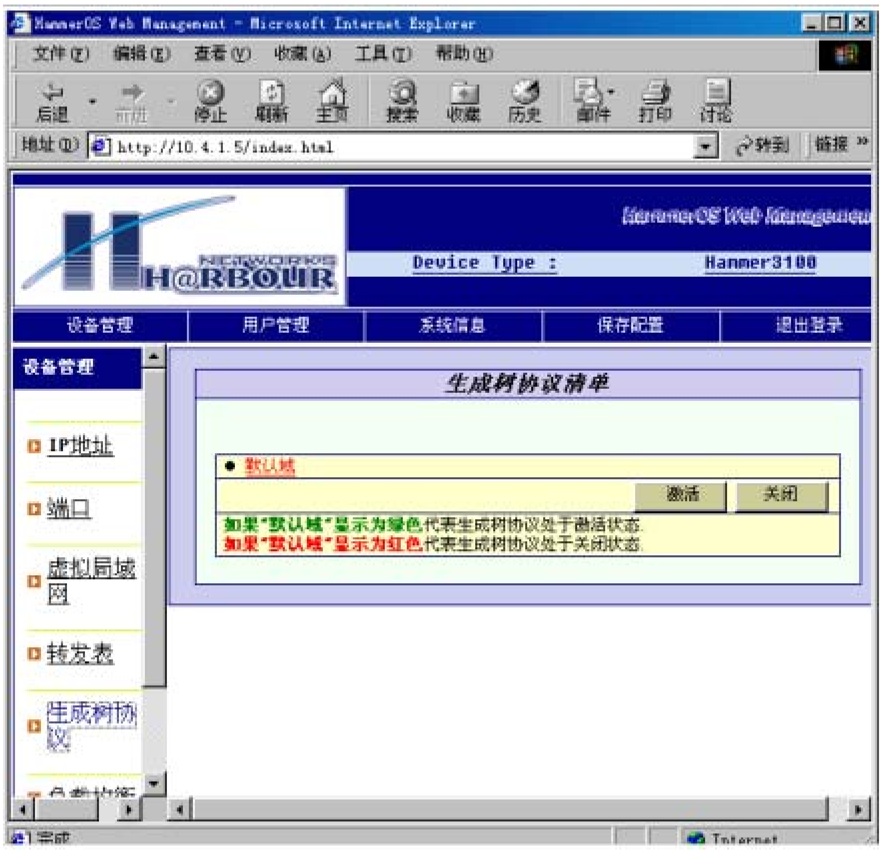


图 11-22 生成树协议 1

在左边 “ **设备管理** ” 栏中点击 “ **生成树协议** ” 如图 11-22 所示，按激活按钮提交，这时默认域字样变成了绿色，表示生成树协议已经激活。而红色代表生成树协议还没有被激活。关闭生成树协议方法与上述操作类似，选择后点击 “ **关闭** ” 按钮。

11.6.3 配置生成树协议的有关参数

单击要配置的生成树协议域项，这里我们选择 “ **默认域** ” 结果如下图 11-23 所示：



图 11-23 生成树协议 2

根据图 11-23 的提示可以填入相应的值。

- 设置运行STP协议时本交换机的优先级
- 优先级Priority的取值范围是0-65535，缺省值为32768。优先级数值越低，越有可能成为网络中的根桥（Root Bridge）。优先级值为0代表了最高的优先级。
- 设置当本交换机被选为根桥时发送BPDU的时间间隔

桥发送 BPDU 时间间隔的取值范围是 0-10，单位为秒，缺省值是 2 秒。

注意：桥发送 BPDU 时间间隔必须小于等于桥切换时间间隔－2

- 设置当本交换机被选为根桥时端口状态切换的时间间隔

桥切换时间间隔的取值范围是 4-30，单位为秒，缺省值为 15 秒。

注意：桥切换时间间隔的时间必须大于等于桥发送 BPDU 时间间隔+2

- 设置BPDU报文老化的最长时间间隔

收到超过这个时间的 BPDU 报文，就直接丢弃。报文老化最大时间间隔的取值范围是 6-40，单位秒，缺省值为 20 秒。

注意：报文老化最大时间间隔的时间必须大于等于 2*(桥发送 BPDU 时间间隔+1)小于等于 2*(桥切换时间间隔–1)

11.6.4 使能 STPD Port

单击图 11-23 所示的相应端口。

例如：单击端口 1，结果如图 11-24 所示：



图 11-24 生成树协议 3

在图 11-24 中，单击“**端口退出 STP 计算**”按钮，则端口 1 不参加计算，反之再重复以上步骤可以使端口 1 使能。

11.6.5 配置 STPD Port 的有关参数

- 配置参与STP计算的端口的优先级Priority

端口优先级的取值范围是 0-255，缺省值是 128。优先级数值越低，端口越容易成为根端口（Root

Port），优先级值为 0 代表了最高的优先级。

- 配置参与STP计算端口的路径开销Path Cost

取值范围是 1-65535，HammerOS 根据端口的当前速率设置不同的缺省值：

1. 10Mbps 端口缺省值为 100
2. 100Mbps 端口缺省值为 19
3. 1000Mbps 端口缺省值为 4

11.7 多端口负载均衡组的配置

多端口负载均衡组(Load Sharing)在 Web Server 中的配置

要设置 Load Sharing，必须创建 Load Sharing 的一组端口。Load Sharing 定义必须遵从以下规则：

- 在一台Hammer3100交换机中只支持一个Load Sharing
- Hammer3100交换机中的一个Load Sharing中最多有4个端口

在主控制页面中左侧的快速链接栏中单击“ 负载均衡 ”进入其控制界面，如图 11-25 所示：



图 11-25 端口负载均衡 1

此时如果已经有 Load Sharing 建立，组内端口中将会显示相对应的端口。

11.7.1 Load Sharing 的创建

创建一个 Load Sharing，按以下步骤进行：

在图 11-25 中，单击“ **创建** ”按钮，开始创建 Load Sharing，如下图 11-26 所示:



图 11-26 端口负载均衡 2

在选择主端口号文本输入中输入要创建 Load Sharing 的主端口，在源和目的下拉列表中选择是否属于源和目的方式创建 Load Sharing，选择 YES 属于这种方式，选择 NO，不属于这种方式，选择端口组成员。

例如：创建的这个 Load Sharing 组的主端口为 9，根据源和目的创建 Load Sharing，成员端口为 1、2、3、9，然后单击“ **OK** ”按钮，出现界面如图 11-27 所示：

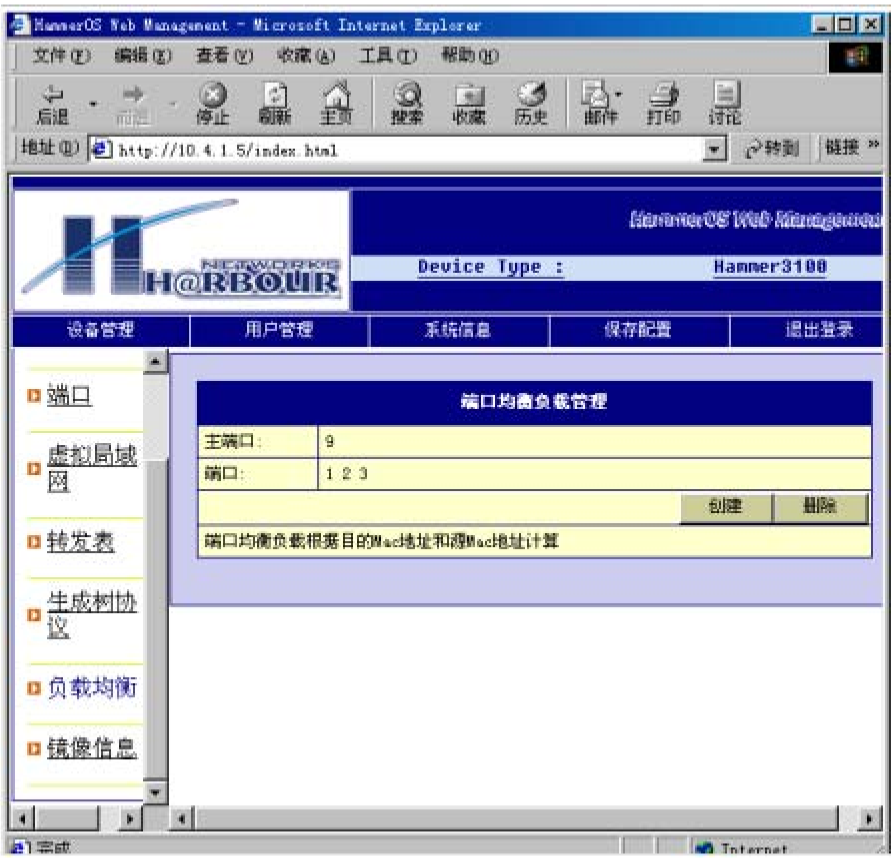


图 11-27 端口负载均衡 3

表明这个 Load Sharing 组已经创建成功。

11.7.2 Load Sharing 的删除

在图 11-25 中，在 Load Sharing 管理表格中，点击 " **删除** " 按钮，即可将 Load Sharing 删除。

⚠ **注意：必须在相互连接的两台交换机上都设置 Load Sharing，且主端口必须对应，否则会在网络中造成回路。**

11.8 镜像信息管理

Hammer3100 系列交换机支持端口镜像，把指定端口或 VLAN 的所有数据报文重定向到镜像端口，以方便错误的诊断。同时，Hammer3100 系列交换机支持通过 Web 来对端口镜像进行管理。

在左边 " **设备管理** " 栏中点击 " **镜像信息** "，出现界面如图 11-28 所示：



图 11-28 镜像信息管理

选择要配置的镜像端口，然后点击“**更新**”按钮，完成操作。

11.9 用户访问权限的设置

HammerOS 中提供了两种用户权限：

- ADMIN 管理员
- NORMAL 普通用户

该用户权限也可以通过 Web 页面来设置。

管理员能进入配置模式并对系统的所有参数进行查看和设置。管理员还能增加、删除用户帐号，设置修改用户密码，在本 Web 的页面管理模块中，包括显示用户列表，增加一个用户，编辑特定用户。点击页面上方的“用户管理”一栏，出现图 11-29：



图 11-29 用户管理 1

11.9.1 增加用户

增加一个用户，可以按照以下步骤进行：

1．以用户名 admin 登录（或者用任何其他管理员的用户帐号登录）；

2．点击页面上方的“ 用户管理 ”进入用户管理界面，如图 11-29 所示。

表格当前系统中的用户列表将显示现在所有的用户名和用户身份，如果以后在其他的界面中，只需点超级链接用户列表即可进入此界面。

击页面左边的“ **增加** ”，即可进入增加用户界面，如图 11-30 所示：



图 11-30 用户管理 2

命名规则：

- 用户名必须为以字母开头的，只包含大写或小写的英文字母、数字、下划线的长度为4-20的字符串。
- 密码可以是由任意字符组成的长度为6-20的字符串。输入并且确认密码之后，点“ 下一步” 按钮。

例如：输入用户名 manager, 密码 harbour；单击“ 下一步 ” 按钮，出现如图 11-31 所示信息：

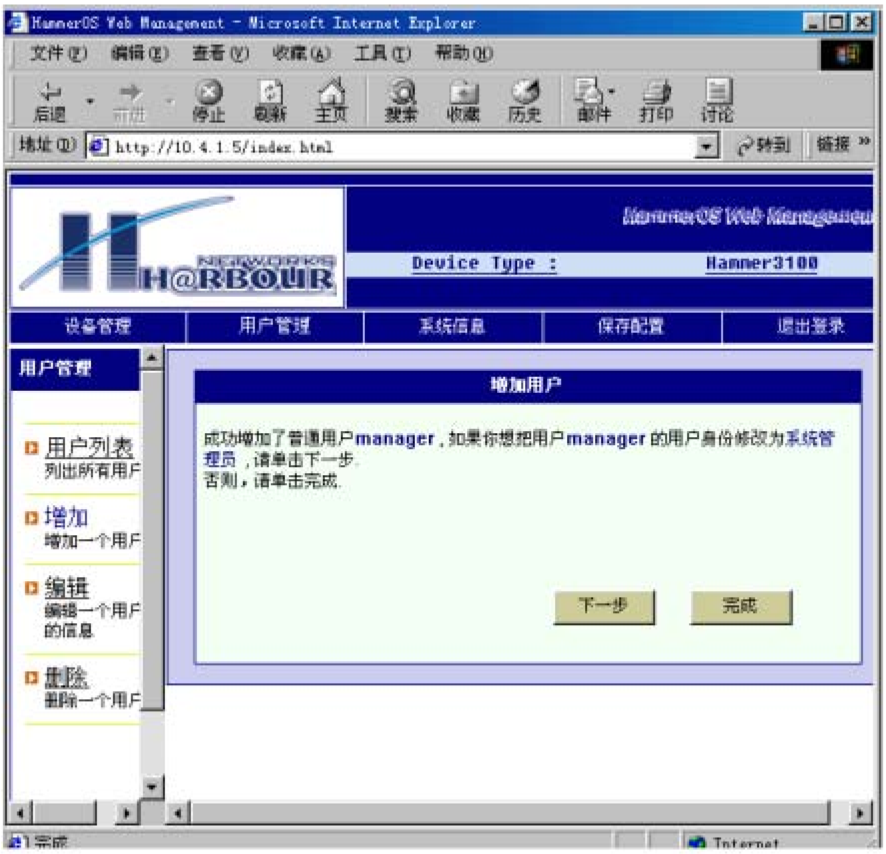


图 11-31 用户管理 3

如图 11-31，显示添加用户成功的信息提示，如果需要添加成为管理员用户可单击“下一步”按钮，否则按完成按钮结束操作。假如选择“下一步”按钮，进入下一个操作界面，如图 11-32 所示。

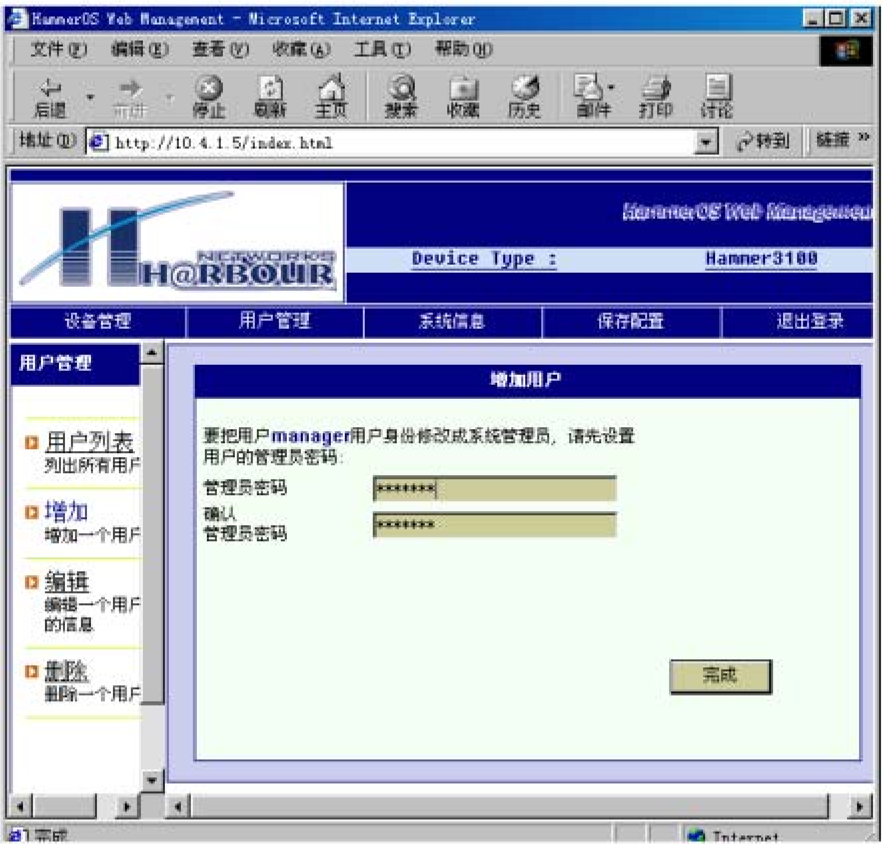


图 11-32 用户管理 4

输入“ 管理员密码和确认密码 ”按下“ **完成** ”按钮结束操作。可以由图 11-33 看出，用户 manager 变为管理员用户。



图 11-33 用户管理 5

注意：系统对于用户名是不区分大小写的，对密码区分大小写。

11.9.2 修改用户

可以使用以下方法把一个用户设为管理员或者是设为普通用户：

在用户管理的快速链接栏中点击“ **编辑** ”,进入编辑用户界面；如图 11-34 所示，选择用户名单击“ **下一步** ”，例如：选择“ admin ”



图 11-34 用户管理 6

单击“下一步”后结果如图 11-35 所示。



图 11-35 用户管理 7

在这个界面中有三个选项：

- 修改用户登录密码
- 修改用户身份
- 修改管理员密码（如果此用户是普通用户将不显示该项）

如果是选择修改密码，系统将提示重新输入密码。如果选择的是修改用户身份，则直接改变当前用户的身份（从普通用户成为管理员身份，需增加输入管理员密码）。

11.9.3 删除用户

在左侧快速连接栏中点击“ **删除** ”，进入删除用户界面，如图 11-36：



图 11-36 用户管理 8

如果选择所要删除的用户姓名为 admin，则出现错误提示，如图 11-37 所示：

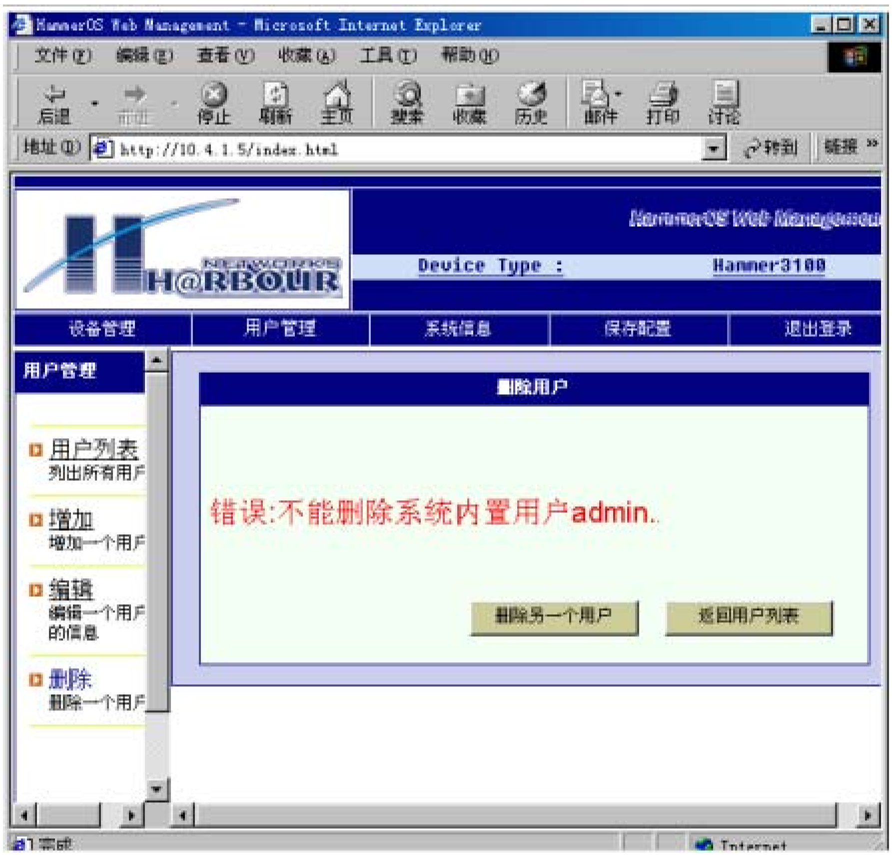


图 11-37 用户管理 9

2．在用户列表中选择要删除的用户再单击“删除”按钮即可。

11.9.4 查看系统信息

选择系统信息将显示如图 11-38 所示界面,它告诉我们有关系统的信息。例如: 产品名称，产品序列号，基 MAC 地址，系统名称，硬件版本号，Bootrom 版本号，软件版本号，生产日期。

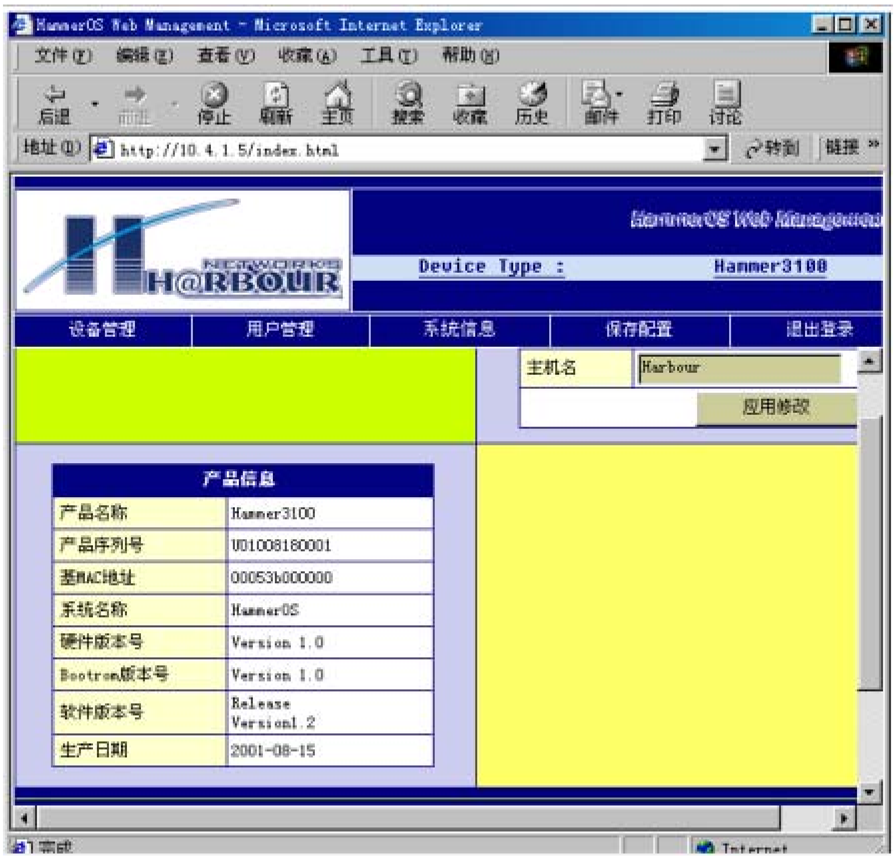


图 11-38 系统信息

11.10 保存配置

单击屏幕菜单栏上的“ **保存配置** ”，出现界面如图 11-39 所示,选择确定保存，即可将配置保存到扩展 Flash 中，保存成功，出现图 11-40。


HammerOS Web Management - Microsoft Internet Explorer
http://10.4.1.5/index.html
Device Type : Hammer3100
设备管理
用户管理
系统信息
保存配置
退出登录
为了保存您对系统配置所做的修改，使得现在运行的配置成为系统每次启动后的缺省配置。
您必须保存配置为系统启动配置。
如果你确定这么做，请单击确定保存按钮。
如果你不是很确定要这么做，请单击取消按钮回到设备管理。
确定保存
取消

图 11-39 保存配置 1


HammerOS Web Management - Microsoft Internet Explorer
http://10.4.1.5/index.html
Device Type : Hammer3100
设备管理
用户管理
系统信息
保存配置
退出登录
正在为保存配置准备数据...完成.
正在把配置文件写入闪存中...完成.
已经成功把配置保存到闪存中.
返回设备管理
完成
Internet

图 11-40 保存配置 2

注意：当您完成所有的配置工作，一定要记住保存配置信息，否则重起之后您将丢失所有您所配置的信息。

11.11 退出登录

当您完成所有的配置您就可以退出了，单击屏幕菜单栏最右边的“**退出登录**”，出现初始的登录界面图 11-1。

第12章 启动选项和软件升级

本章包括如下内容：

- Bootrom启动选项介绍
- 升级HammerOS软件
- 重新启动交换机

12.1 Bootrom 启动选项介绍

Bootrom 启动分成两种方式：

- 自动启动
- 人工干预启动

12.1.1 自动启动

在默认方式下，交换机在上电之后，用户不需要干预，交换机将进入直接启动模式，进入 HammerOS 操作系统中。启动成功后，对于 Hammer3100 系列交换机显示操作系统界面如下：

```
Hammer Boot Loader version 1.0, Harbour Networks, Inc.

Compiled Wed 28-FEB-2001 11:00

Base ethernet MAC address: 00:05:3b:01:36:00

Copyright(c) 2000-2001 by Harbour Networks, Inc.

Product name: MicroHammer VDSL Switch
Serial number: U51001080003
Manufacture date: 2001-08-01
Hardware revision: version 1.00

System booting, please wait...

Open console ...... Done.
Entering HammerOS ......

Initializing environment ...... Done.
Loading startup config ...... Done.
```

```
##############################################################
#                                                            #
#                    Welcome to HammerOS.                    #
#                                                            #
#       Press Return to connect and config this system.      #
#                                                            #
##############################################################
```

然后按回车键，进行用户登录。

12.1.2 人工干预启动

按照以下步骤可以访问 Bootrom 菜单：

1．连接交换机的 Console 端口，注意终端的正确配置。

2．使能交换机电源，并且不停的按空格键。

3．当出现“ Hammer: ”提示符，说明已经进入 Bootrom 菜单。

人工干预启动后显示 Bootrom 菜单信息如下：

```
Hammer Boot Loader version 1.0, Harbour Networks, Inc.

Compiled Wed 28-FEB-2001 11:00

Base ethernet MAC address: 00:05:3b:01:36:00

Copyright(c) 2000-2001 by Harbour Networks, Inc.

Product name: MicroHammer VDSL Switch
Serial number: U51001080003
Manu
 ?                - List all available commands
 h                - List all available commands
 b                - Boot an executable image
 g                - Boot an executable image with default configurations
 u                - Load and boot an executable image
 l                - Load configuration file and boot an executable image
 r                - Reboot system


Press 'h' or '?' To get helping information.
Hammer:
```

Bootrom 菜单选项及其含义如下：

?：显示所有的命令信息

h：显示所有的命令信息

b：直接执行 HammerOS

g：使用缺省配置执行 HammerOS

u：使用 Xmodem 协议下载 HammerOS，并执行

l：使用 Xmodem 协议下载配置文件，并执行 HammerOS

r：重新启动交换机

注意：下载的 HammerOS 存储到 Flash 中。HammerOS 的软件升级功能既提供 Xmodem 下载，又提供 FTP 下载，并保存到 Flash 中。

12.2 升级 HammerOS 软件

HammerOS 提供了两种升级软件的方式：

- 通过串口用Xmodem协议下载HammerOS
- 通过TCP/IP网络用FTP协议下载HammerOS

12.2.1 通过串口用 Xmodem 协议下载新版 HammerOS

按以下步骤通过串口下载 HammerOS：

1．使用有管理员权限的用户通过串口登录，并进入配置模式；

2．输入命令

Harbour(config)# download xmodem hammeros

3．使能串口超级终端的发送文件菜单，选择 HammerOS 可执行文件，选择发送；

4．下载完毕后，输入 reboot 命令重新启动交换机。

提示：如果想了解详细的操作步骤请参照本手册 2.5 节相关内容。

12.2.2 通过 TCP/IP 网络用 FTP 协议下载新版 HammerOS

按以下步骤通过 FTP 下载新版的 HammerOS：

1．使用有管理员权限的用户通过串口或者 TCP/IP 网络登录，并进入配置模式；

2．输入命令：

【命令语法】download ftp hammeros <A.B.C.D> <username> <password> <filename>

【参数说明】

参数	说明
A.B.C.D	hammeros 文件所在机器的 IP 地址
username	FTP 的用户名
password	该用户的密码
filename	所要下载的文件名

3．等待系统完成 FTP 下载和写入 Flash；

4．完毕后，输入 reboot 命令重新启动交换机。

系统显示：

```
System is going to reboot....
Disconnected.
Thanks for using Harbour Networks's product.
Bye!
```

提示：如果想了解详细的操作步骤请参照本手册 2.5 节相关内容。

12.2.3 重新启动交换机

当您需要重新启动交换机时，可以使用 reboot 命令。

使用此命令重新启动交换机之前，请考虑是否需要保存配置数据。如果需要保存配置数据，请键入如下命令：

```
Harbour(config)# save configuration
```

该命令完成保存配置数据的操作。

感谢您对港湾网络有限公司产品的支持和信赖，如果您有好的意见和建议，请给我们发邮件 customer@harbournetworks.com，或登录我们的网站 www.harbournetworks.com 跟我们联系，我们将认真对待您的意见和建议。